

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001 年 11 月 1 日 (01.11.2001)

PCT

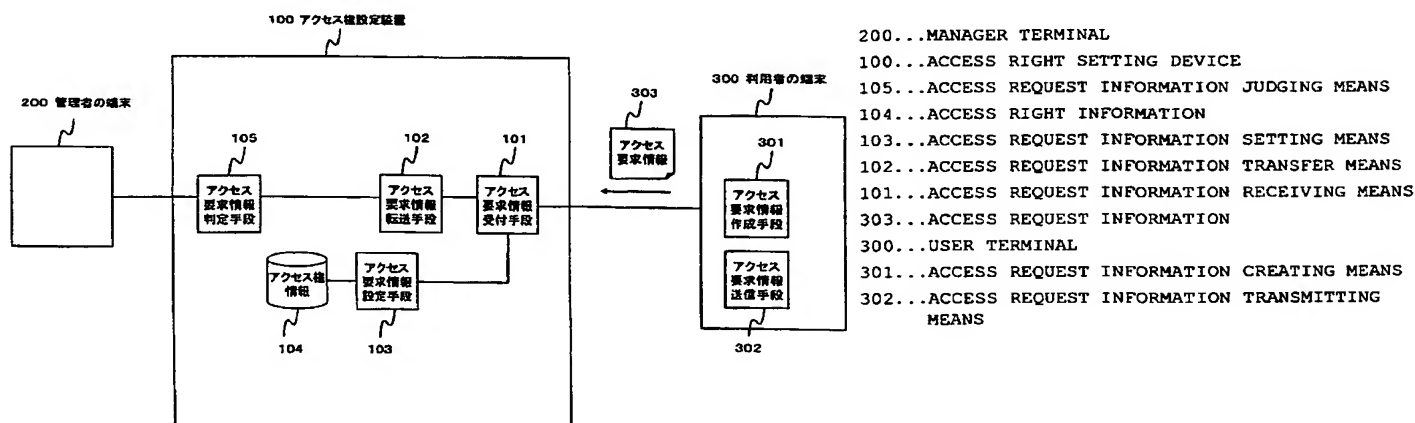
(10) 国際公開番号
WO 01/82086 A1

- | | | |
|---|---------------------------------|--|
| (51) 国際特許分類: | G06F 12/00, 13/00, 15/00 | [JP/JP]; 干 819-1112 福岡県前原市浦志 482-1-202 Fukuoka (JP). |
| (21) 国際出願番号: | PCT/JP01/03515 | |
| (22) 国際出願日: | 2001 年 4 月 24 日 (24.04.2001) | (74) 代理人: 二瓶正敬(NIHEI, Masayuki); 干 160-0004 東京都新宿区四谷2丁目12-5 第6富沢ビル6階 Tokyo (JP). |
| (25) 国際出願の言語: | 日本語 | (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW. |
| (26) 国際公開の言語: | 日本語 | |
| (30) 優先権データ:
特願2000-122681 | 2000 年 4 月 24 日 (24.04.2000) JP | (84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). |
| (71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 干 571-0000 大阪府門真市大字門真1006番地 Osaka (JP). | | |
| (72) 発明者; および | | |
| (75) 発明者/出願人 (米国についてのみ): 上田真臣 (UEDA, Masaomi) [JP/JP]; 干 336-0015 埼玉県浦和市太田窪2012-2 Saitama (JP). 石川 晃 (ISHIKAWA, Akira) [JP/JP]; 干 214-0022 神奈川県横浜市多摩区堀2-12-3 301 Kanagawa (JP). 三藤 隆 (MITOH, Takashi) | | |
| | | 添付公開書類:
— 国際調査報告書
— 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。 |

[続葉有]

(54) Title: ACCESS RIGHT SETTING DEVICE AND MANAGER TERMINAL

(54) 発明の名称: アクセス権設定装置及び管理者端末



(57) Abstract: An access right setting device for readily setting an access right when a user of which the access to a resource of a network is limited makes a request and a system including a manager terminal are disclosed. In the system, a user who requests an access to a resource describes the contents of setting of an access right such as the resource, time, and access content in access request information (303) and sends it to an access right setting device (100) managing an access right, the received access request information (303) is transferred to the manager of the resource by an access request information transfer means (102), the manager confirms the content of the request and makes a judgement of approval, and thus the access right setting device (100) automatically sets an access right.

〔統葉有〕

WO 01/82086 A1



2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

ネットワークの資源へのアクセスを制限された利用者が要求を出すことで、簡単にアクセス権の設定が行えるアクセス権設定装置及び管理者端末を含むシステムが開示され、同システムでは、資源へのアクセスしたい利用者が、資源、時間、アクセス内容などのアクセス権の設定内容をアクセス要求情報 3 0 3 に記述し、アクセス権を管理するアクセス権設定装置 1 0 0 へ向けて送信する。受け取ったアクセス要求情報 3 0 3 は、アクセス要求情報転送手段 1 0 2 により、資源の管理者へ転送され、管理者が要求内容を確認し承認の判断を下すだけで、アクセス権設定装置 1 0 0 により自動でアクセス権の設定が行われる。

明 細 書

アクセス権設定装置及び管理者端末

5 技術分野

本発明は、ネットワーク上に存在する制限的に利用可能な資源を利用する利用者からの要求によるアクセス権の設定が可能なアクセス権設定装置及びそのシステムに関する。

10 背景技術

従来、ネットワーク上の資源を複数の利用者がアクセスする場合、その資源を管理しているコンピュータに、利用者のアクセス権の情報が保持されており、この情報を基にアクセス制御を行うことになる。ここで、利用者とは、人間、プログラム、プロセス（実際は、人間がプログラム
15 やプロセスを作成し実行することになる）などを表し、資源とは、ファイル、メモリ、プログラム、プロセス、機器などを表す。

アクセス権情報は一般的に、各利用者単位、又は、利用者が属するグループ単位で、参照（資源の存在の確認）、読み出し（資源の内容を見る）、書き込み（資源の内容を書き変える）、消去（資源を記録媒体から消去す
20 る）、実行（プログラムを実行する）などのアクセス形態に関し、アクセスを許可するか否かの記述をする。

一般的なネットワークOS（オペレーティング・システム）でのアクセス権の設定方法を説明する。ネットワークの管理者により、ユーザ（利用者）に対し、ネットワークへアクセスするのに必要なユーザID（利
25 用者識別子）の登録が行われ、リモート・アクセスの許可設定を行うことで、アクセスが可能となる。その他、ネットワークの管理者は、アク

セス期間や、ユーザのグループ化なども設定できる。ユーザがアクセス可能な資源は、主に自らが管理しているマシン内の資源や、それぞれのマシンの管理者が外部ユーザからのアクセスを許可した資源などである。

- このようなアクセス権の設定内容は、通常資源の管理者が設定を行う
5 もので、資源の利用者は設定できない。もし資源の利用者がアクセス権のない資源へアクセスする場合は、何らかの手段でアクセス権変更の要求を管理者に伝えることになる。

- 又、ネットワークのユーザIDを持っていないユーザがアクセスする手段として、ゲストIDという概念がある。一般的に、ゲストIDでネ
10 ットワークへログインするために必要なパスワードは公知であり、だれでもネットワークへアクセスできるのだが、セキュリティ上、ネットワークに障害が起きないように、アクセス可能な資源が極めて限定されている。いずれにしても、利用者がアクセス権の設定をすることはできない。

- 15 利用者が管理者へネットワーク経由でアクセス要求を伝え、アクセス権の設定を行う方式として、特開平5-006322号公報がある。利用者がアクセス権を有しない資源へのアクセスを行った場合、アクセス権の変更依頼が管理者へ通知され、管理者がアクセスを許可するようなアクセス権の変更を行う、といったアクセス権の設定方式である。

- 20 本発明では、特に一般の家庭で構築される、ネットワーク家電機器を繋いだホームネットワークでの実現を考える。通常ホームネットワークで資源（ネットワーク家電機器）を管理する管理者（家庭の人）は、ネットワークの知識がない人が多く、複雑な条件のアクセス権の設定の処理が困難であると言える。又、資源の利用者としては、家庭内の人
25 はもちろんだが、外部の事業者がサービスを提供するために資源を利用する場合が考えられる。サービス例としては、遠隔医療、遠隔監視、遠隔保

守などが挙げられる。上述の通り、管理者である家庭の人はアクセス権の設定が困難なため、利用者である外部の事業者がアクセス権の設定内容を提示し、家庭の人はアクセス権情報として登録するかの判断、又は簡単な作業を行うのみ、という簡易な設定方式を考える。

- 5 以上のようなホームネットワークを利用した上で、従来の技術における課題を挙げる。

第1の課題として、アクセス権の設定内容（アクセス権を適用する期間、アクセス内容、その他アクセスできる条件など）の指定を、管理者ではなく利用者の方で行うことができない。

- 10 第2の課題として、アクセス権設定の要求は、利用者主導でアクセス権を管理している装置へ送信しなければならない。

第3の課題として、アクセス権の管理をするのは人間でなければならず、その場にいない場合はアクセス権の設定処理が滞り、又、頻繁にアクセス権設定の要求が投げられる場合は面倒である。

- 15 第4の課題として、利用したい資源（以下、アクセス対象資源という）を保持するネットワークに対して、資源へアクセスするための通信ができない（以下、ログインできないという）利用者は、アクセス権設定の要求を出すことができない。又、管理者は、ログインするためのユーザIDの設定という特殊な知識が必要になる。

- 20 第5の課題として、利用者が、利用したい資源を一意に特定する識別子を知らない場合、アクセス要求情報に、アクセスを許可して欲しいアクセス対象資源を指定することができない。

第6の課題として、第3の課題を解決した場合、指定されたアクセス対象資源を、利用者側で選択することができない。

- 25 第7の課題として、第1の課題を解決した場合、利用者によるアクセス権の設定内容の指定はできるが、更に、管理者により詳細な指定を行

いたい場合もでてくる。

第 8 の課題として、利用者が、ネットワークにどういう資源が存在するか知りたい場合がある。

第 9 の課題として、第 1 の課題を解決した場合、利用者がアクセス要求情報を不正に作成することで、管理者（人間）へ表示した内容とは別の設定が行われる可能性がある。

第 10 の課題として、第 1 の課題を解決した場合、利用者が指定したアクセス権の設定内容が信頼できるものか、客観的な判断が難しい。

第 11 の課題として、管理者の端末が携帯端末である場合でも、第 1 又は、第 2 の課題を解決したい。

第 12 の課題として、管理者の端末が携帯端末である場合でも、第 6 の課題を解決したい。

第 13 の課題として、管理者の端末が携帯端末である場合でも、第 7 の課題を解決したい。

15

発明の開示

本発明は、以上の課題を解決するために、ネットワークのユーザ ID を持たない利用者により、存在や識別子を知らないネットワークの資源に対して、アクセス権の設定内容（以下、利用者がアクセス権の設定要求のために指定するアクセス権の設定内容を「アクセス要求情報」と言う）を指定を行うものである。これにより、管理者に負担をかけずにアクセス権の設定が可能になり、又、利用者、並びにアクセス要求情報が信頼でき、管理者に知られずに不正にアクセス権の変更が行われなくとも実現する。さらに、管理者により、利用者が指定したアクセス要求情報の変更が行えるしくみも実現する。

20
25

なお、特開平 5 - 0 0 6 3 2 2 号公報記載のアクセス権の設定方式で

は、利用者が利用したい資源の識別子を知らない場合や、利用者がネットワークのユーザIDを持たない場合の解決手段について言及していない。又、管理者により詳細なアクセス権の設定が行われるが、利用者にはそのアクセス権の指定内容が制限されている。

- 5 この課題を解決するために本発明は、第1に利用者が指定したいアクセス要求情報を作成する手段と、利用者が指定したアクセス要求情報を受け取る手段と、アクセス要求情報を管理者へ転送する手段と、アクセス要求情報を基に管理者が設定の可否判定を行う手段と、管理者の許可判断により、利用者が指定したアクセス要求情報をアクセス権情報として
- 10 設定する手段とを備えたことにより、管理者によるアクセス権の複雑な設定が必要なくなると共に、利用者によるアクセス権の設定内容の指定が可能となる。

- 第2に、利用者が、作成したアクセス要求情報を管理者側から見える場所に一旦保存する手段と、管理者側からこのアクセス要求情報を取得
- 15 する手段を備えたことにより、管理者主導でアクセス権の設定が容易にできる。

- 第3に、アクセス要求情報をアクセス権情報として設定するかの可否判定を機械により自動で行う手段を、管理者の端末に備えたことにより、人間が、利用者の端末にいない場合でも、機械が自動で判定を行い、又、
- 20 アクセス要求情報が頻繁に投げられる場合のような煩わしい作業も、機械での自動化で解消できる。

- 第4に、ネットワークへログインする際のユーザ認証で必要な利用者のユーザIDを作成し、アクセス権情報の一部として登録する手段を備えたことにより、ネットワークへログインできず、ユーザIDを持たない
- 25 利用者からでも、管理者へアクセス権設定の要求が可能となる。

第5に、利用者、管理者双方で既知である、資源を抽象化した種別情

報でのアクセス対象資源の記述が行えることにより、ネットワークへログインできない利用者などが具体的な資源の識別子を知らない場合でも、アクセス権設定の要求が可能になる。

第6に、第3の解決手段で記載した、利用者が利用したいアクセス対象資源を種別の情報で指定した場合に、管理者により利用を許可する資源を選択する手段を備えたことにより、アクセス対象資源を一意に決定できるのと共に、管理者の意志が尊重されたアクセス権の設定が可能となる。

第7に、アクセス要求情報を転送する手段で管理者に提示されたアクセス要求情報に記述された内容を、管理者からも変更ができる手段を備えたことにより、利用者だけに一方的にアクセス権の設定内容が指定されることなく、管理者の意志が尊重された、より柔軟なアクセス情報の設定が可能になる。

第8に、ネットワークが備えたアクセス可能な資源の情報を、利用者が取得できる手段を備えたことにより、資源の識別子を知らない利用者でも、資源の存在や、その情報を取得することができ、アクセス要求情報へ盛り込むことが可能となる。

第9に、利用者が作成したアクセス要求情報を基に、人間である管理者に提示する自然言語による表示情報を作成する手段を備えたことにより、悪意のある利用者が不正に作成したアクセス要求情報にて、不正にアクセス権を設定されることなく、正確にアクセス要求情報の内容を管理者へ伝えることが可能となる。

以下、機械が理解できるように人間によって作られたプログラムやコードなどの表現を人工言語、人間が理解できる、音声、画像、文字などのUI（ユーザ・インターフェース）情報の元となる表現を自然言語と呼ぶ。

第10に、受け取った、信頼のおけるCA（認証局）によるデジタル署名が施されてるアクセス要求情報の認証を行う手段を備えたことにより、利用者、又はアクセス要求情報が信頼のおけるもので、且つ改ざんや、なりすましの恐れがないかの判断が可能となる。

5 第11に、携帯端末へ受け取ったアクセス要求情報を転送する手段と、アクセス要求情報をアクセス権情報として設定してもよいかの可否判定を、携帯端末にて行うことができる手段をアクセス権設定装置に備えたことにより、管理者が管理者の端末にいない、外出をしているような場合でも、容易にアクセス権の設定を行うことが可能となる。

10 第12に、利用者が、利用したいアクセス対象資源を種別の情報で指定した場合、携帯端末にて利用を許可する資源を選択する手段をアクセス権設定装置に備えたことにより、管理者が管理者の端末にいない、外出をしているような場合でも、容易に対象資源の選択を行うことが可能となる。

15 第13に、携帯端末用のアクセス要求情報を転送する手段で管理者に提示されたアクセス要求情報の内容を、携帯端末にて変更ができる手段を備えたことにより、管理者が管理者の端末にいない、外出をしているような場合でも、容易にアクセス要求情報に記述されている内容の変更を行うことが可能となる。

20

図面の簡単な説明

図1は、本発明の第1の実施の形態におけるアクセス権設定システムの全体構成を示す図、

図2は、図1のアクセス要求情報の一例を表す図、

25 図3は、本発明の第1の実施の形態におけるアクセス権設定の一連の動作例を表すシーケンス図、

図 4 は、本発明の第 1 の実施の形態における判定画面の一例を表す図、
図 5 は、本発明の第 1 の実施の形態における判定結果の通知画面の一例を表す図、

図 6 は、本発明の第 1 の実施の形態におけるアクセス権設定の一連の
5 動作例を表すフローチャート図、

図 7 は、本発明の第 2 の実施の形態におけるアクセス権設定システムの全体構成を示す図、

図 8 は、図 7 のアクセス要求情報の一例を表す図、

図 9 は、本発明の第 2 の実施の形態におけるアクセス権設定の一連の
10 動作例を表すシーケンス図、

図 10 は、本発明の第 2 の実施の形態におけるサービス一覧画面の一例を表す図、

図 11 は、本発明の第 3 の実施の形態におけるアクセス権設定システムの内、管理者の端末の構成を示す図、

図 12 は、本発明の第 3 の実施の形態におけるアクセス権設定の一連の動作例を表すフローチャート図、
15

図 13 は、本発明の第 4 の実施の形態におけるアクセス権設定システムの全体構成を示す図、

図 14 は、図 13 のアクセス要求情報に記述するアクセス対象資源の種別情報の一例を表す図、
20

図 15 は、本発明の第 4 の実施の形態におけるアクセス権設定の一連の動作例を表すシーケンス図、

図 16 は、本発明の第 5 の実施の形態におけるアクセス権設定システムの内、管理者の端末の構成を示す図、

図 17 は、本発明の第 5 の実施の形態におけるアクセス権設定の一連の動作例を表すシーケンス図、
25

図 1 8 は、本発明の第 5 の実施の形態におけるアクセス要求情報の内容表示画面の一例を表す図、

図 1 9 は、本発明の第 5 の実施の形態における選択画面の一例を表す図、

5 図 2 0 は、本発明の第 6 の実施の形態におけるアクセス権設定システムの全体構成を示す図、

図 2 1 は、図 2 0 の公開資源情報の一例を表す図、

図 2 2 は、図 2 0 の公開資源の種別情報の一例を表す図、

10 図 2 3 は、本発明の第 6 の実施の形態におけるアクセス権設定の一連の動作例を表すシーケンス図、

図 2 4 は、本発明の第 7 の実施の形態におけるアクセス権設定システムの全体構成を示す図、

図 2 5 は、本発明の第 7 の実施の形態における不正に作成されたアクセス要求情報の一例を表す図、

15 図 2 6 は、本発明の第 7 の実施の形態における変換テーブルの一例を表す図、

図 2 7 は、本発明の第 7 の実施の形態におけるアクセス権設定の一連の動作例を表すシーケンス図、

20 図 2 8 は、本発明の第 7 の実施の形態におけるアクセス権設定の一連の動作例を表すフローチャート図、

図 2 9 は、本発明の第 8 の実施の形態におけるアクセス権設定システムの全体構成を示す図、

図 3 0 は、本発明の第 8 の実施の形態におけるアクセス権設定装置と携帯端末間の一連の動作例を表すシーケンス図である。

以下、本発明の実施の形態について、図 1 から図 30 を用いて説明する。なお、本発明はこれら実施の形態に何ら限定されるものではなく、その要旨を逸脱しない範囲において、種々なる態様で実施し得る。

(実施の形態 1)

- 5 図 1 は、本発明のアクセス権設定装置及び管理者端末を含むネットワークシステム全体の第 1 の実施の形態の構成を表すものである。第 1 の実施の形態では、アクセス権の設定内容を利用者が指定できると共に、管理者はその指定内容で適切なものか判別するだけで、簡易にアクセス権の設定を行えるようにするのが目的である。
- 10 本発明のネットワークシステムは大きく、アクセス権設定装置 100、管理者の端末 200、利用者の端末 300、といった装置群から構成される。アクセス権設定装置 100 は、管理している資源へのアクセスを制限するためのアクセス権の設定及び管理を行う装置である。管理者の端末 200 は、利用者から要求されるアクセス権の設定内容の確認及び
- 15 アクセス権の設定を行うための管理者用の端末である。なお、管理者の端末 200 はリモートの端末と限定せず、アクセス権設定装置 100 そのものと考えてもよいものとする。利用者の端末 300 は、利用者がアクセス権設定の要求を出したり、実際にアクセスする際に用いる端末である。利用者の端末 300 を用いてアクセスする利用者からは、アクセス
- 20 権設定装置で管理されているネットワーク資源へ自由にアクセスできるわけではなく、アクセス権情報 104 に基づいたアクセス制御により、利用者からのアクセスが制限されることになる。なお、これらの端末群及び装置は同一機器としてもよく、その形態は特に限定しない。また、アクセス権設定装置 100 にて管理されるアクセス権を用いてのアクセス
- 25 制御が行われる場所も、アクセス設定装置 100 のみならず、特に限定しない。なお、本発明で用いる利用者とは、人間とは限らず、機械が

自動で動く場合でもよいものとする。

まず、利用者の端末 3 0 0 内の構成要素について説明する。アクセス要求情報作成手段 3 0 1 は、利用者が利用したい資源へのアクセスを許可してもらうための要求情報であるアクセス要求情報 3 0 3 を作成する
5 手段である。このアクセス要求情報 3 0 3 は、アクセス要求情報送信手段 3 0 2 にて、アクセス権設定装置 1 0 0 へ送信されることになる。

次に、アクセス権設定装置 1 0 0 内の各構成要素について説明する。アクセス要求情報受付手段 1 0 1 は、利用者が作成したアクセス要求情報 3 0 3 を受け付けるための手段である。アクセス要求情報転送手段 1
10 0 2 は、アクセス要求情報受付手段 1 0 1 で受け付けたアクセス要求情報 3 0 3 の内容を管理者の端末へ転送する手段である。なお、内容の転送は図 1 のようにリモートの端末だけではなく、アクセス権設定装置 1 0 0 内のローカルでの転送でもよく、以後ローカル転送の例を説明する。アクセス要求情報設定手段 1 0 3 は、管理者がアクセス要求情報の内容
15 を許可した場合に、アクセス権情報 1 0 4 として設定を行うための手段である。

アクセス要求情報判定手段 1 0 5 は、アクセス権設定装置 1 0 0 のアクセス要求情報転送手段 1 0 2 により転送されたアクセス要求情報 3 0 3 の内容を、アクセス権情報 1 0 4 として設定するかどうかの判定を行
20 うための手段である。この手段で設定が許可されれば、アクセス要求情報設定手段 1 0 3 により、アクセス権情報 1 0 4 として設定されることになる。なお、アクセス要求情報判定手段 1 0 5 は、アクセス権設定装置 1 0 0 ではなく、リモートの端末にあってもよいものとする。

利用者により作成されるアクセス要求情報 3 0 3 の一例を図 2 に示す。
25 アクセス要求情報 3 0 3 は、利用者とアクセス権設定装置 1 0 0 同士で通信を可能にするため、双方で理解し得る共通の通信規約（プロトコル）

に則って作成されるものであり、コンピュータが理解できる人為的に作られた例えばXML (Extensible Markup Language) のような人工言語として記述される。

図2に示される各項目の説明を行う。「利用者」はネットワークを利用
5 する利用者を一意に識別する識別子(ネットワークのユーザIDのことを言う)を表し、利用者がネットワークへのアクセスを許可されているかどうかの判断(ユーザ認証)を行う場合、又は管理者へどの利用者からの要求かを通知したい場合などに用いられる。「利用端末」は、利用者が資源へアクセスする際に使用する端末の場所(ネットワークアドレス)
10 を表しており、該当する端末からのみアクセス可能と、制限を加える場合に用いる。「期間」は、アクセスが可能となる期間を表し、期間の制限を加えたい場合に用いる。「アクセス対象資源」は、利用者がアクセスを許可して欲しい資源を表す。「アクセス内容」は、利用者がアクセスを許可して欲しい内容を表す。以上の項目から、利用者によるアクセス権の
15 設定内容の指定が可能となる。図2で挙げた項目は一例であり、この他に必要な項目があれば、アクセス要求情報の一部として追加しても構わないものとする。又、図2記載の項目は任意であり、すべてが必要という訳ではない。

以上のように構成されたネットワークシステムにおける、アクセス権
20 設定装置及びそのシステムについて、その動作を説明する。

図3に、アクセス権設定装置100、管理者の端末200、利用者の
端末300間での動作例を示す。利用者が、アクセス要求情報作成手段
301により、前記通信規約に則って、アクセス要求情報303が作成
される(1001)。利用者によって作成されたアクセス要求情報303
25 は、アクセス要求情報送信手段302により、アクセス権設定装置100
0へ向けて送信される。ここで、アクセス権設定装置100へ送信する

際に必要なアドレスなどの情報は、利用者側であらかじめ既知であるものとする。送信されたアクセス要求情報 3 0 3 は、アクセス権設定装置 1 0 0 のアクセス要求情報受付手段 1 0 1 により受け付けられる。アクセス要求情報 3 0 3 を単独で送信してもよいし、アクセス権設定装置 1 0 0 内で動作させるためのアプリケーション・プログラムなどと一緒に送信してもよいものとする。なお、アクセス要求情報受付手段 1 0 1 は、アクセス要求情報 3 0 3 に記載された通信規約を知っており、理解することができるものとする。ただし、アクセス要求情報 3 0 3 は、不正にアクセス権情報 1 0 4 として設定されないように、信頼のおける情報とする (1 0 0 2)。

受け取ったアクセス要求情報 3 0 3 は、アクセス要求情報受付手段 1 0 1 からアクセス要求情報転送手段 1 0 2 に渡され、アクセス要求情報判定手段 1 0 5 へその内容が転送される。アクセス要求情報転送手段 1 0 2 は、あらかじめ転送先を知っているものとし、ネットワークで繋がっていて転送可能であれば、コンピュータ、ネットワーク家電など、種類、及び数量は特に限定しない。なお、特にあらかじめ転送先を知らなくても、利用者がアクセス要求情報 3 0 3 に転送先 (管理者の指定、又は転送端末の指定) を記述することで、転送先の指定も可能とする (1 0 0 3)。

転送されたアクセス要求情報 3 0 3 の内容は、アクセス権設定装置 1 0 0 のアクセス要求情報判定手段 1 0 5 により、アクセス権情報 1 0 4 として設定するかどうかの判定が行われる。判定は管理者である人間により行われるもので、例えば、管理者の端末 2 0 0 上に、アクセス要求情報 3 0 3 の内容が表示され、その表示内容を参照し判定を行うことになる。なお、表示形式としては、利用者がアクセス要求情報に盛り込んだ、文字、音声、画像などの、人が理解し易い自然言語の表示形式、又

は、機械向けの人工言語の内容をそのまま表示することになる。

図 4 に、管理者の端末 2 0 0 に表示される判定画面の例を示す。図 4 は、図 2 に示すアクセス要求情報 3 0 3 の内容を表示したもので、文字及びボタンなどの UI（ユーザー・インターフェース）情報を用いた自然言語による表現となる。

この自然言語は、利用者によりアクセス要求情報の一部として記述されるか、又は別に画面表示用のプログラムを用意するなどして表示される。管理者としては、表示された内容に対して許可判定を行う（図 4 の例では、許可、不許可のどちらかのボタンを押す作業）だけなので、アクセス権の細かな指定をする必要がなくなり、簡易に設定を行うことができる。ただし、利用者の身元及びアクセス権の指定内容は、あまり知識のない管理者では判定が難しいかもしれないので、この場合は、熟練した専門家に判定を依頼するような、判定代行のモデルも考えられる（1 0 0 4）。アクセス要求情報 3 0 3 が許可された場合、その情報がアクセス権設定装置 1 0 0 のアクセス要求情報受付手段 1 0 1 まで返る（1 0 0 5）。判定結果を受けたアクセス要求情報受付手段 1 0 1 はアクセス要求情報設定手段 1 0 3 へアクセス権情報 1 0 4 への設定を依頼することで、結果としてアクセス要求情報 3 0 3 が、アクセス権情報 1 0 4 として設定される（1 0 0 6）。無事に設定された旨を、設定内容と共に、利用者の端末へ通知する。

図 5 に、利用者への通知画面の例を示す。なお、図 5 のようにアクセス権の設定内容の詳細まで通知しなくてもよく、設定可否の旨だけを通知してもよい（1 0 0 7）。

以下に説明する構成要素は図 1 に示していないが、設定されたアクセス権情報 1 0 4 を基に、どのようにアクセス制御が行われるかの説明を行う。なお、例としてアクセス制御はアクセス権設定装置 1 0 0 内で行

われているとするが、特にアクセス制御が行われる場所は問わない。まず、利用者の端末から対象資源へのアクセスが起こる。なお、1002のアクセス要求の動作で説明した通り、アクセス要求情報303は、アクセス権設定装置100内で動作するアプリケーション・プログラムなど
5 と送信してもよく、この場合は、アクセス制御による資源の利用制限を受ける利用者をアプリケーション・プログラムに置き換えることができる(1008)。アクセス権情報104として設定されているユーザID情報を基に、利用者がネットワークへのアクセスを許可されているかどうかの判断であるユーザ認証を行う。認証の手段としては、パスワード
10 ドを利用した手段などが考えられる(1009)。アクセス権情報104として設定された、「利用端末」、「期間」、「アクセス対象資源」、「アクセス内容」などを基に、アクセス権設定装置100により、アクセス対象資源へのアクセス可否の判定をするアクセス権のチェックが行われる(1010)。この結果、アクセスが許可された場合には、対象資源への
15 アクセスが可能となる(1011)。

図6に、アクセス権の設定が行われるまでのフローチャートを示す。利用者が作成したアクセス要求情報303を受け付ける(1101)。アクセス要求情報303を理解し、管理者の端末200へ転送する(1102)。管理者がアクセス要求情報303の許可判定を行う(1103)。
20 許可された場合は、アクセス要求情報303を設定し(1104)、その結果が利用者へ通知される(1105)。許可されない場合は、アクセス要求情報303は設定されず(1106)、不許可の結果が利用者へ通知される。図6に利用者への通知の例を示す(1107)。

上述のように構成された本発明の第1の実施の形態によれば、従来は
25 管理者によって決められていたアクセス権が、利用者によって指定できるようになり、逆に、管理者は煩わしいアクセス権の設定がなくなって、

管理者の負担が軽減される。特に、ネットワーク対応の家電・AV機器を繋いで構成されるホームネットワークについて考えると、管理者である家庭の人はネットワークの知識があまりないことから、アクセス権の設定が簡易に可能になる本発明は有効な方式であると言える。又、ホームネットワークと外部のインターネット網とを接続することで、不特定多数の利用者から、頻繁に複雑な設定が必要とされる点が考えられ、有効なシステムであるといえる。

(実施の形態2)

図7は、本発明第2の実施の形態におけるネットワークシステム全体の構成を表すものである。第2の実施の形態では、利用者の端末からアクセス要求情報を送信しなくても、アクセス権設定装置側からアクセス要求情報を取得することを目的とする。

図1に示す第1の実施の形態では、利用者の端末300からアクセス要求情報303を送信し、アクセス権設定装置100へ伝えていたが、本実施の形態では管理者の依頼により、アクセス権設定装置100が、ある場所に保存されているアクセス要求情報303を取得しにいく手段を備えた点が異なる。

本実施の形態の構成を図7を用いて説明する。ただし、実施の形態に記載のネットワークシステムと同様に、アクセス権設定装置100、管理者の端末200、利用者の端末300にて構成されており、一部の機能は同じものであるので、異なる点についてのみ説明する。なお、以下管理者の端末200はリモートの端末と限定せず、アクセス権設定装置100そのものと考えてもよいものとする。

利用者の端末300には、アクセス要求情報作成手段301により作成したアクセス要求情報303を保存するために用いるアクセス要求情報保存手段304を備える。保存先として、利用者の端末から通信可能

なネットワーク上にアクセス要求情報蓄積装置 400 が存在する。アクセス権設定装置 100 には、アクセス要求情報蓄積装置 400 に蓄積されているアクセス要求情報 303 を取得し、受け付けるために用いるアクセス要求情報受付手段 101 を備える。又、アクセス権設定装置 100 には、アクセス要求情報 303 の取得処理をアクセス要求情報判定手段 105 へ依頼するアクセス要求情報取得依頼手段 114 を備える。なお、アクセス要求情報取得依頼手段 114 は、アクセス権設定装置 100 ではなく、リモートの端末にあってもよいものとする。

ホームネットワークには、ネットワークに対応した家電・AV 機器が接続されており、この機器を外部から制限的に利用可能な資源と仮定する。利用者を警備会社とし、ホームネットワークに接続されているビデオカメラへアクセスすることで、留守宅の映像を取得する遠隔監視サービスの例を考える。この例は言い換えれば、ホームネットワークへサービスを提供していると言うことができる。一般的に、ホームネットワークの管理者（家庭の人を意味する）は、コンピュータ及びネットワークの知識を有していないと考えられ、複雑なアクセス権の設定は困難である。又、提供されるサービスも多種多様であり、ホームネットワークの家庭の人とは異なる部外者（コンピュータネットワークで言うところのゲスト）が資源の利用者となり、より一時的なアクセスが要求される。

以上の点からも、ホームネットワークへサービスを提供する利用者（事業者）へのアクセス権の付与を考えた場合、通常のコンピュータネットワークのアクセス権の設定よりも多種多様な用途が考えられ、更に複雑な設定が必要となる。従って、第 1 の実施の形態に記載の、「管理者に複雑な設定を行わせず」に、「利用者によるアクセス権の設定内容の指定が可能」な、アクセス権の設定のしくみの必要性が高まると言える。

ホームネットワークへ提供されるサービスの一例として、上述した警

備会社による遠隔監視サービスを用いて以下説明する。

遠隔監視サービスの場合のアクセス要求情報 3 0 3 の例を図 8 に示す。

「利用者」は、利用者を特定するための識別子であるユーザ ID を示しており、ネットワークへログインする際の認証時に利用者を識別するために用いられるものである。警備会社 A が複数のサービスを提供する場合も考えらるので、利用者を識別するユーザ ID を、利用者毎というよりは、サービス毎に作成した方が望ましい。「属性」は、利用者、又はサービスが属するグループを示しており、グループ単位でのアクセス制御を行う場合に必要となる。「利用端末」、「期間」、「アクセス内容」は、第 1 の実施の形態での説明と同じであるため、ここでは省略する。「アクセス対象資源」は、利用者が利用したい資源を表しており、ここで「ビデオカメラ B」は、ホームネットワークに接続されている機器を一意に特定できる識別子（ネットワークアドレス、具体的な資源名など）を指定して表している。最後に「条件」は、その他の時間的に変化の伴う要因に依存したアクセス権情報 1 0 4 で、例えば「警報センサ反応時」の場合は、侵入物によるセンサ反応時のみ監視を行わせるためにアクセスを許可し、それ以外の正常時にはアクセスを許可しないといった、詳細で柔軟な設定も可能になる。

以上のように構成されたネットワークシステムにおける、アクセス権設定装置及びそのシステムについて、その動作を説明する。

図 9 に、アクセス権設定装置 1 0 0、管理者の端末 2 0 0、利用者の端末 3 0 0、アクセス要求情報蓄積装置 4 0 0 間での動作例を示す。この例では、アクセス要求情報判定手段 1 0 5、及びアクセス要求情報取得依頼手段 1 1 4 が管理者の端末 2 0 0 にある場合として説明する。図 9 は、図 1 に示す第 1 の実施の形態における動作例に新たな動作 1 2 0 2 ~ 1 2 0 5 を加えたものであり、残りの 1 2 0 1 は、1 0 0 1 に、1

206～1213は1004～1011にそれぞれ対応しているため、ここでは説明を省略する。

利用者がアクセス要求情報作成手段301にて作成したアクセス要求情報303を、アクセス要求情報保存手段304を用いてアクセス要求
5 情報蓄積装置400へ保存する(1202)。

なお、アクセス要求情報蓄積装置400は、利用者の端末300及びアクセス権設定装置100から通信可能であればよく、特に設置されている場所は限定しない。管理者は、管理者の端末200からアクセス権設定装置100のアクセス要求情報取得依頼手段114へアクセスし、
10 アクセス権設定装置100のアクセス要求情報取得手段へ向けて、アクセス要求情報蓄積装置400に蓄積してあるアクセス要求情報303の取得の依頼を行う。なお、管理者は、アクセス要求情報蓄積装置400に存在するアクセス要求情報303の一覧を見るなどして、あらかじめ取得したいアクセス要求情報303を知っているものとする。

15 図10にホームネットワークに導入するサービス一覧画面の例を示す。各サービスに対応するアクセス要求情報303が、アクセス要求情報蓄積装置に存在することを意味する。図10の例で、もし管理者である家庭内の人、サービス一覧から遠隔監視サービスを選択した場合、遠隔監視サービスのアクセス要求情報303を取得するための依頼コマンド
20 が、アクセス権設定装置100のアクセス要求情報取得手段まで投げられることになる(1203)。管理者から依頼されたアクセス要求情報受付手段101は、該当するアクセス要求情報303をアクセス要求情報蓄積装置400から取得する。この際、アクセス要求情報303を単独で取得してもよいし、アクセス権設定装置100内で動作させるための
25 アプリケーション・プログラムなどと一緒に取得してもよいものとする。

アプリケーション・プログラムと一緒に取得した場合、アクセス要求

情報 3 0 3 に記述されたアクセス権設定の内容は、利用者及びアプリケーション・プログラムに対する利用したい資源へのアクセス権の内容となる (1 2 0 4)。アクセス要求情報受付手段 1 0 1 は、取得したアクセス要求情報 3 0 3 をアクセス要求情報転送手段 1 0 2 へ渡され、管理者
5 の端末 2 0 0 へその内容が転送される (1 2 0 5)。

上述のように構成された本発明の第 2 の実施の形態によれば、利用者がアクセス権設定の要求を投げることなく、管理者側からアクセス要求情報を取得できることで、上述のホームネットワークのサービスを導入する例のように、管理者が希望するときに、簡易にアクセス権の設定を
10 行うことが可能になる。又、利用者から一方的に送信されることなく、管理者の意思に従ってアクセス要求情報を取得しにいくので、不正アクセスを招く可能性が低くなるという効果もある。

(実施の形態 3)

図 1 1 は、本発明第 3 の実施の形態におけるネットワークシステム全体の構成のうち、新たに手段を追加した管理者の端末の構成を表すものである。第 3 の実施の形態では、管理者が人間ではなく、機械により自動で、アクセス要求情報をアクセス権情報 1 0 4 として設定するかの可否判定を行うことを目的とする。
15

図 1 に示す第 1 の実施の形態におけるアクセス権設定装置 1 0 0 の構成と異なり、図 1 1 では、機械によりアクセス要求情報をアクセス権情報 1 0 4 として設定する可否判定を行うアクセス要求情報自動判定手段 2 0 3 を管理者の端末 2 0 0 に備えている。
20

以上のように構成されたネットワークシステムにおける、アクセス権設定装置及びそのシステムについて、その動作を説明する。

25 図 1 2 に、アクセス権の設定が行われるまでのフローチャートを示す。アクセス要求情報 3 0 3 を受け付ける及び取得する動作は、第 1 及び第

2の実施の形態にて説明した通りであるので、ここでは説明を省略する。

アクセス要求情報303を管理者の端末へ転送する(1301)。転送する際、判定モードの確認を行う(1302)。この判定モードは、人間による判定と機械による判定のどちらで行うかを示しているもので、管理者によりあらかじめ設定されているものとする。なお、設定がされていない場合でも、デフォルト値があらかじめ設定されているものとする。

5 もし判定モードが自動であれば、アクセス要求情報自動判定手段203にてアクセス要求情報303の可否判定が行われる。機械による判定の場合は、判定基準となるアルゴリズムが、あらかじめアクセス要求情報自動判定手段203に登録されていることになり、このアルゴリズムにより、転送されてきたアクセス要求情報303に記述されている内容を把握し、自動でアクセス権情報104として設定するかの可否判定が行えるものとする(1303)。なお、この判定基準となるアルゴリズムについては特に限定しないので、ここでは触れない。

10 もし判定モードが自動でない場合は、アクセス要求情報判定手段201にてアクセス要求情報303の可否判定が行われる(1304)。仮に、管理者が端末にログインしていない場合、又は端末が起動していなかった場合などのように、管理者が判定をできる状態ではないとアクセス権設定装置100が判断できれば、判定の処理をアクセス要求情報自動判定手段203に切り替える処置を取ってもいいものとする。

15 アクセス要求情報判定手段201による可否判定処理は第1の実施の形態で説明しているので、ここでは省略する。又、アクセス要求情報自動判定手段203及びアクセス要求情報判定手段201の双方で判定した結果の処理1305～1308は、第1の実施の形態の図6のフローチャートの1104～1107にて説明している

20 25

上述のように構成された本発明の第3の実施の形態によれば、アクセ

ス要求情報に記述された内容をアクセス権情報として設定するかの可否判定を、機械により自動で行うことにより、管理者が端末にいない場合でも自動でアクセス権の設定が行える。又、複雑なアクセス権の内容のアクセス要求情報を頻繁に判定しなければならない場合には、判定を自動モードに切り替えることにより、管理者に手間がかからずにアクセス権の設定を行うことも可能になる。

(実施の形態 4)

図 1 3 は、本発明第 4 の実施の形態におけるネットワークシステム全体の構成を表すものである。第 4 の実施の形態では、ネットワークへログインすることのできない利用者からでも、アクセス権設定の要求を受け付け、ログインするために必要な利用者を一意に確定する識別子（以下、ユーザ ID と言う）を発行することを目的とする。

図 1 に示す第 1 の実施の形態の構成図と異なり、図 1 3 に示すネットワークシステムでは、ローカルネットワーク 5 0 0 にログインするために必要なユーザ ID を持たない利用者（の端末）からのアクセス要求を考え、アクセス権設定装置 1 0 0 内に、利用者の識別子（ユーザ ID）を発行し、アクセス権情報 1 0 4 の一部として登録する利用者識別子登録手段 1 0 6 を備えている。なお、管理者の端末 2 0 0 及び利用者の端末 3 0 0 の構成は変わっていない。

以下、分かり易く説明するために、ローカルネットワーク 5 0 0 の例として、第 3 の実施の形態でも触れたホームネットワークの遠隔監視サービスの例を用いて説明をする。

外部のネットワークと接続されているホームネットワークは、外部からの不正アクセスを防ぐためにアクセス権の設定によるアクセス制御、又は、アクセスの拒否などの制限が必要である。以下、図 1 3 に示すローカルネットワーク 5 0 0 をホームネットワークと置き換え、外部のネ

- ットワークの利用者が利用者の端末 300 を用いてホームネットワークの資源を利用すると考える。つまり、外部の利用者が、遠隔監視サービスを提供する警備会社とする。サービスを導入する前の警備会社は部外者であり、通常ホームネットワークへのログイン及び資源へのアクセス
- 5 が許可されておらず、ホームネットワークへログインするためのユーザ ID を持っていない状態であるといえる。利用者からの要求によるアクセス権の設定を実現するためには、このようなユーザ ID をあらかじめ持っていない利用者からでも、アクセス要求情報 303 によるアクセス権の設定要求が行える枠組みをつくる必要がある。
- 10 利用者がネットワークのユーザ ID を持っていない部外者である場合、ネットワークにログインできずに、ネットワークがどういう資源を保持しているのか分からないケースが多いといえる。つまり、ネットワークを一意に特定する識別子が分からないことになるので、図 8 に示すように、アクセス要求情報 303 に記述するアクセス対象資源を指定することができない。この問題を解決するために、アクセス対象資源の識別子を抽象化した種別の情報で指定可能とする。分かり易い例として、ホームネットワークに対応したビデオカメラの指定の仕方を図 14 に示す。
- 15 「アクセス対象資源」を「ビデオカメラ全部」、「ビデオカメラ 1 台」、「Panasonic 製のビデオカメラ」のように抽象化して種別（以下、種別情報という）での指定を行うものとする。ただし、利用者側で指定された資源が、管理者（アクセス権設定装置）側で理解されなければいけないため、種別情報による指定は、その資源の表記が規格化され一般的に（又は、利用者と管理者の間で）認知されている場合に用いることができる。例えば、あるホームネットワークの規格では、ビデオカメラはあるコードで規格化されているので、利用者が記述した資源のコードを管
- 20 理者側で理解することができ、アクセス要求情報 303 の一記述形態と

して用いることができる。但し、ホームネットワーク内に、例えば「ビデオカメラB」、「ビデオカメラC」というように、複数の同一規格の機器が存在する場合は、「ビデオカメラ全部」の指定では2台のビデオカメラともアクセス権設定の対象になり、「ビデオカメラ1台」の指定では、
5 どちらか1台が対象となり、その対象を決定するアルゴリズムは特に限定しない。

以上のように構成されたネットワークシステムにおける、アクセス権設定装置及びそのシステムについて、その動作を説明する。

図15に、アクセス権設定装置100、管理者の端末200、利用者
10 の端末300間での動作例を示す。この例では、アクセス要求情報判定手段105が管理者の端末200にある場合として説明する。図15は、図3に示す第1の実施の形態における動作例に新たな動作1406～1408を加えたものであり、残りの1401～1405は、1001～1005に、1409～1412は1008～1011にそれぞれ対応
15 しているため、ここでは説明を省略する。なお、1402でのアクセス要求で、利用者がアクセス権設定装置100のアクセス要求情報受付手段101へ要求を送信する場合は、ユーザIDを持たない利用者からでもアクセス要求情報受付手段101にて受け付け可能とする。

管理者の端末200からアクセス権設定装置100内のアクセス要求
20 情報判定手段105を用いて、管理者に許可されたアクセス要求情報303は、アクセス権情報104として設定されるが、利用者はネットワークのユーザIDを持っていないため、アクセス権情報104の一部として、ユーザIDの登録が必要になる。このユーザIDは、次回資源へアクセスする際に、ユーザ認証を受けログイン可能とするために必要と
25 なる。又、アクセス制御を行う際、このユーザIDをキーにしてアクセス権の確認を行う際にも必要になる。アクセス権設定装置100内の利

用者識別子登録手段 106 は、アクセス要求情報 303 の「利用者」の
情報、又は独自の方式で利用者の識別子（ユーザ ID）を決定し、ア
クセス権情報 104 の一部として登録する。この際、管理者は特にユーザ
ID の作成を意識することなく、利用者識別子登録手段 106 により自
5 動で行われてもよいし、管理者自らユーザ ID を決定してもよい（14
06）。アクセス要求情報設定手段により、アクセス要求情報 303 が、
アクセス権情報 104 として設定される（1407）。無事に設定された
旨を、設定された内容、ユーザ ID と共に（もしパスワードによってユ
ーザ認証を行う場合は、パスワードも）、利用者の端末へ通知する（14
10 08）。

上述のように構成された本発明の第 4 の実施の形態によれば、従来は
ネットワークのユーザ ID を持たない利用者からはネットワークにログ
インできず、アクセス要求を行う解決策が存在していなかったが、本発
明により課題が解決されることで、サービスを提供する部外者からの一
15 時的なアクセスが考えられるホームネットワークでは、特に効果的であ
ると言える。又、通常管理者によりユーザ ID を決定し登録する煩雑な
作業も無くなる。更に図 14 に示すように、アクセス対象資源を規格化
されたコードで指定ができるので、利用者は資源の識別子情報を知る必
要がなくなり、管理者も利用者に識別子を伝える必要がなくプライバシ
20 ーの保護に役立つといった効果がある。

（実施の形態 5）

図 16 は、本発明第 5 の実施の形態におけるネットワークシステム全
体の構成を表すものである。第 5 の実施の形態では、利用者により指定
されたアクセス要求情報に対して、管理者でも変更を可能にし、又、利
25 用者がアクセス対象資源を種別情報で指定した場合でも、管理者が複数
のアクセス対象資源の中からアクセス対象資源を決定することを目的と

する。

図 1 6 に示す構成図は、図 1 1 に示す第 3 の実施の形態の構成図に新たな構成を加えたものである。第 3 の実施の形態の構成とは、管理者の端末 2 0 0 内に、利用者が作成したアクセス要求情報 3 0 3 を管理者の都合のいいように変更することが可能なアクセス要求情報変更手段 2 0 5 と、利用者が資源の種別情報でアクセス対象資源を指定し、該当する資源のうちどれにアクセス権を与えるか選択することが可能なアクセス対象資源選択手段 2 0 4 を備えた点が異なる。

10 以上のように構成されたネットワークシステムにおける、アクセス権設定装置及びそのシステムについて、その動作を説明する。

図 1 7 に、アクセス権設定装置 1 0 0、管理者の端末 2 0 0、利用者の端末 3 0 0 間での動作例を示す。図 1 7 は、図 1 5 に示す第 2 の実施の形態における動作例に、新たな動作 1 5 0 4 ~ 1 5 0 7 を加えたものであり、残りの 1 5 0 1 ~ 1 5 0 3 は、1 4 0 1 ~ 1 4 0 3 に、1 5 0 8 ~ 1 5 1 4 は、1 4 0 6 ~ 1 4 1 2 にそれぞれ対応しているため、こ
15 こでは説明を省略する。

利用者により作成されたアクセス要求情報 3 0 3 が、管理者の端末 2 0 0 へ転送される。転送されてきたアクセス要求情報 3 0 3 に対して変更が必要な場合は、アクセス要求情報変更手段 2 0 5 にて変更を行う。

20 例として、第 2 の実施の形態にて説明を行った図 8 に示すアクセス要求情報 3 0 3 が転送された場合について説明する。管理者が人の場合は、管理者の端末 2 0 0 に表示されるアクセス要求情報 3 0 3 の内容を確認し、「期間」、「アクセス対象資源」、「アクセス内容」、「条件」の変更、追加、削除などを行うことが可能である。図 1 8 に管理者の端末 2 0 0 に
25 アクセス要求情報 3 0 3 に記述された内容の表示画面の例を示す。管理者は、画面の変更ボタンを押すことで、アクセス要求情報変更手段 2 0

5 にて、各アクセス要求情報の内容の変更が可能になる。変更は、利用
者と管理者が相互に交渉しながら行う形態でもよい（1504）。もし、
利用者がアクセス対象資源を規格化された資源の種別情報で指定した場
合、複数の資源がアクセス対象資源として設定されることになる。利用
5 者は、利用したい資源の識別子が分からないために資源の種別情報を用
いてアクセス対象資源を指定していると考えられるので、指定された種
別に当てはまる全ての資源をアクセス対象資源として許可するというこ
とは、本来利用を許可する資源以外のものも許可してしまう恐れもあり、
アクセス範囲を広げてしまうかもしれないという問題が発生する。そこ
10 で管理者の意思で、利用者からの利用を許可する資源の選択を行うのが
望ましい。アクセス対象資源を資源の種別情報にて記述した例を挙げる。
単純に「ビデオカメラ」と指定された場合は、管理者の判断で利用を許
可する資源を選択する必要がある。なお許可する数量は特に限定しない。
「ビデオカメラ全部」という指定の場合は、特に管理者が利用を許可す
15 る資源を選択しなくても、該当するビデオカメラを全てアクセス対象資
源となる（実際には、全ての資源の識別子がアクセス権情報のアクセス
対象資源として登録される）。状況に応じて利用を許可する資源を絞り込
んで選択してもよい。「ビデオカメラ1台」という指定の場合は、どのビ
デオカメラの利用を許可するか選択しなければならない。図19に「ビ
20 デオカメラ1台」と指定された場合の、アクセス対象資源の選択画面の
例を示す。アクセス対象資源選択手段204により、指定された種別情
報に該当する資源がピックアップされる。

管理者はこの中からアクセスを許可する資源を1つ以上選択する。た
だし許可しない場合は選択しなくてもよい。なお、選択を自動化するた
25 めに、あらかじめ選択される資源の優先度の指定を行ってもよいものと
する（1505）。管理者が、アクセス権の設定を許可する判定を行う（1

- 506)。アクセス要求情報303が許可された場合、その情報がアクセス権設定装置100のアクセス要求情報受付手段101まで返る。但し、1504にて要求情報の変更を行っている場合は、変更した情報が返り、更に1505にてアクセス対象資源の絞込み選択を行っている場合は、
- 5 選択されたアクセス対象資源の識別子情報も返る(1507)。なお、1504の変更処理、1505の選択処理及び1506の判定処理の順序は特に限定しない。又、ホームネットワークの家庭の人が管理者だと仮定すると、あまり知識がないことから、1506のアクセス要求情報303の判定が、困難になるかもしれない。この場合は、1506の判定
- 10 処理は専門家(設定代行業)に委託し、1504の変更処理及び1505の選択処理は、家庭内の人が行う、といった処理の分担を行ってもよい。すなわち、アクセス要求情報判定手段201、アクセス要求情報変更手段205及びアクセス対象資源選択手段204は同一端末上ではなく、分散環境としても構わないものとする。
- 15 上述のように構成された本発明の第5の実施の形態によれば、利用者により指定されるアクセス要求情報303を、管理者の意志で柔軟に設定できる。又、資源の識別子を知らない利用者が、資源の種別情報を用いてアクセス対象資源の指定を行った場合でも、管理者により利用を許可する資源の選択を行うことで、余計なアクセス対象資源の設定を防ぐ
- 20 ことができる。特にホームネットワークの例のように、ネットワークの知識が乏しい管理者であっても、簡易にアクセス権の設定内容の変更及びアクセス対象資源の指定ができ、効果的であるといえる。

(実施の形態6)

- 図20は、本発明第6の実施の形態におけるネットワークシステム全体の構成を表すものである。第6の実施の形態では、ネットワークのログインできない利用者のように、ネットワークに存在する資源の識別子
- 25

及びネットワークに存在する資源の種別情報を知らない場合に、これらの情報の取得を可能にすることを目的とする。

図 1 3 に示す第 4 の実施の形態の構成図と異なり、図 2 0 に示す構成では、ローカルネットワーク 5 0 0 で保持している資源の識別子情報、
5 又は種別情報の中で、外部のネットワーク向けに公開している情報と、この公開している情報を取得する公開資源情報取得手段 3 0 5 を利用者の端末 3 0 0 に備えている。なお、管理者の端末 2 0 0 の構成は変わっていない。

公開資源情報記憶装置に 1 0 7 に記憶されている情報の例を図 2 1 に
10 示す。公開資源情報記憶装置に 1 0 7 に記憶されている情報は、管理者の意志により、自由にログインできない、ユーザ ID を持たない利用者向けに公開している情報であり、ローカルネットワーク 5 0 0 内の資源の識別子及び種別の一覧情報である。この情報は、必ずしもすべての資源の情報でなく、管理者が外部のネットワークへ公開してもよいと判断
15 した資源やそのアクセス内容に限っているものとする。言い換えると、管理者があまり外部へ公表したくない資源に関しては、公開しなくてもよいといえる。

特に図 2 1 では、ホームネットワークの機器の例として、対象資源の項目で、ビデオカメラが 2 台、デジタルテレビが 1 台あることを表して
20 おり、それぞれ機器（資源）を一意に特定できる識別子の情報である。アクセス内容の項目では、それぞれの機器でアクセス可能な内容であることを表している。図 2 2 は図 2 1 の公開資源情報記憶装置に 1 0 7 に記憶されている情報を抽象化した例を示している。図 2 2 では、機器（資源）の識別子ではなく、種別の情報であるので、仮にビデオカメラが複
25 数台存在する場合でも、1 通りの表現で表されることになる。なお、この公開資源情報記憶装置に 1 0 7 に記憶されている情報は、管理者及び

利用者からの通信が可能であれば、特に存在する場所は限定しない。

通常、管理者からの告知がない限り、資源の存在を知ることが困難なネットワークにログインできない利用者でも、利用者の端末 300 内の公開資源情報取得手段 305 を用いて公開資源情報記憶装置に 107 に
5 記憶されている情報を取得することができる。取得した公開資源情報記憶装置に 107 に記憶されている情報は、アクセス要求情報 303 として、利用したい資源やアクセス内容を指定するときに用いることができる。

以上のように構成されたネットワークシステムにおける、アクセス権
10 設定装置及びそのシステムについて、その動作を説明する。

図 23 に、アクセス権設定装置 100、管理者の端末 200、利用者の端末 300 間での動作例を示す。この例では、図 16 に示す管理者の端末 200 を利用するものとして説明する。図 18 は、図 13 に示す第 4 の実施の形態における動作例に新たな動作 1601、1602 を加えたものであり、残りの 1603～1615 は、1502～1514 に対応しているため、ここでは説明を省略する。
15

ネットワークへログインできない利用者、又はネットワークの資源の情報を知らない利用者が、利用者の端末 300 内の公開資源情報取得手段 305 を用いて、公開資源情報記憶装置 107 から資源の識別子、又は種別情報などの情報を取得する。もし、公開資源情報記憶装置 107
20 がアクセス権設定装置 100 内に存在する場合でも、ネットワークへログインするために必要なユーザ ID を持たない利用者から、ある通信規約（プロトコル）を用いてアクセスできるものとする（1601）。取得した公開資源情報記憶装置 107 に記憶されている情報を基にアクセス
25 対象資源を指定ができるので、結果として利用者の端末 300 内のアクセス要求情報作成手段 301 を用いて、アクセス要求情報 303 を作成

することが可能となる（１６０２）。

上述のように構成された本発明の第６の実施の形態によれば、資源の識別子を知らない場合でも、オンラインで即時に情報を取得することができる。特にネットワークのユーザＩＤを持たずログインできない利用者
5 者は、あらかじめ資源の識別子を知らないことがほとんどであると考えられる。この点からも、識別子情報及び種別情報の取得は有効な手段であるといえる。

（実施の形態７）

図２４は、本発明第７の実施の形態におけるネットワークシステム全
10 体の構成を表すものである。第７の実施の形態では、利用者が作成したアクセス要求情報３０３が信頼のおけるものかの確認と、管理者である人間に知られないように、不正にアクセス権の設定を行わせないようにすることが目的となる。

図２０に示す第６の実施の形態の構成図と異なり、図２４に示す構成
15 では、アクセス権設定装置１００内に、利用者が作成したアクセス要求情報３０３が、信頼できる情報かどうかの認証を行うアクセス要求情報認証手段１０８と、利用者が作成したアクセス要求情報に記述された内容を、人が視覚的に理解し易い自然言語へと変換し表示情報を作成する表示情報作成手段１０９を備えている。なお、管理者の端末２００及び
20 利用者の端末３００の構成は変わっていない。

以上のように構成されたネットワークシステムにおける、アクセス権設定装置及びそのシステムについて、その動作を説明する。

まず第１に、アクセス要求情報３０３が信頼のおける情報かを認証する仕組みを説明する。

25 例としてホームネットワークに導入するサービスを考えた場合、第３者により作成されているものであれば、すべてのサービスが信頼できる

訳ではなく、中には不正行為を働くサービスも存在するかもしれない。信頼できるサービスかの判断を行う手段として、デジタル署名の仕組みがあり、本実施の形態では、この仕組みを利用し、サービスの信頼性を確認する。

- 5 以下、例として公開鍵暗号方式を利用したデジタル署名の基づく、ユーザ認証について説明する。デジタル署名の仕組みをアクセス要求情報 303 に利用すると、不正利用者が名前を偽る「なりすましの防止」、不正利用者によるアクセス要求情報 303 の書き換えなどの「改ざんの防止」、又は、利用者が公的な認証機関によって認証された事実による「信頼度の向上」などを図ることができる。

- 10 まず「なりすましの防止」の説明を行う。利用者が作成したデジタル署名を施したアクセス要求情報 303 を不正利用者が何らかの手段で入手し、これを送信した場合を考える。通常管理者が入手した利用者の公開鍵を利用して、間違いなく利用者から送信されたもののかのユーザ認証
15 を行う。しかし、この場合、不正利用者はユーザ認証を行う際に必要な、利用者の公開鍵のペアとなる秘密鍵を持っていないため、ユーザ認証が失敗する。従って、なりすましを防止することができる。

- 20 次に「改ざんの防止」の説明を行う。利用者が作成したデジタル署名を施したアクセス要求情報 303 を不正利用者が何らかの手段で入手し、これを改ざんを行った場合を考える。本当は利用者の秘密鍵で暗号化しなければならないところ、不正利用者は、この秘密鍵を持っていないため、別の秘密鍵で暗号化するしかない。しかし、管理者は利用者の公開鍵にて復号化を行い、うまくアクセス要求情報 303 が復号化できず、不正に改ざんされたことが分かる。従って、改ざんを防止することが
25 できる。

最後に「利用者の信頼度の向上」の説明を行う。信頼のできる第3者

認証機関であるCA（Certification Authority：認証局）を利用する例である。なお、CAは公正、中立な立場であり、絶対的に信頼できる機関であることが前提となる。利用者は、自分専用の公開鍵、秘密鍵のペアを自ら作成するかCAで作成してもらい、それをCAへ登録申請する。

- 5 このとき、CAにより利用者の身元照会が行わる。CAは利用者の身元照会により登録を許可すると、利用者の公開鍵をCAのデータベースに登録し保管する。そして、登録者の情報をCAの秘密鍵で暗号化した証明書を利用者に渡す。すなわち、この証明書がCAの公開鍵で復号化できれば、CAに認定された信頼のおける利用者と判断することができる。

- 10 第2に、管理者である人間に知られないように、不正にアクセス権の設定を行わせないようにする仕組みを説明する。

まず課題を分かり易く説明する。例として第3者が作成したソフトを、自分のコンピュータで実行する場合を考える。人に見える動作としては、画面に表示されている映像や音があるが、これ以外の人に見えないところ

- 15 るでは、ソフトが何を行っているか分からない。つまり、人に見える範囲では特に問題ないような動きをし、人に見えないところで気付かれないように、不正にアクセス権の設定を行うようなソフトを作成することが可能である。本発明の内容で具体的な例として、悪意のある利用者が、特に問題のない表現で記述された人間が理解し易い自然言語情報と、不正
- 20 正を働く記述がされた人工言語情報とでアクセス要求情報303を作成し、管理者に不正であることを気付かせずにアクセス要求情報303を許可させ、人工言語で記述された不正な内容でアクセス権の設定を行えることが挙げられる。

利用者が不正に作成したアクセス要求情報303の例を図25に示す。

- 25 図25では例として、アクセス要求情報303に人工言語、自然言語を記述しており、人工言語をXMLにて記述している。ここで問題になる

のは、機械が理解できる人工言語では、資源を利用できる「期間」が「2000/1/1～2000/2/29」、「アクセス対象資源」が「0x0004 (=ビデオカメラ)」(図 2 6 の変換テーブル記載のコードの定義を参照)、「アクセス内容」が「0x1020 (=すべての動作)」となっているが、一方、管理者で
5 ある人が理解できる自然言語では、それぞれ「1999/12/1～2000/5/31」、「ビデオカメラ」、「映像取得」と異なった内容の記述がされている。本来、人工言語と自然言語は同じ意味の記述をしなければならないが、この例だと、利用者が管理者を騙して、不正なアクセス権の設定を行う可能性があると言える。

- 10 一旦不正にアクセス権が設定されると、資源への不正アクセスが起こる恐れがあり、セキュリティ上問題になる。第 2 の実施の形態などで説明したホームネットワークで導入するサービスの例だと、当然すべてが信頼できるサービスとは言えず、中には不正な設定を行い、家庭の機器へ不正にアクセスしたり、家庭の情報を盗み出すサービスが存在する可
15 能性もあり、これを解決する仕組みが必要となる。なお、管理者が機械の場合は、もともと自然言語を理解することができないため、この仕組みは適用できない。

このような不正行為を防止するためには、必ずしも信頼できないので利用者が作成した自然言語情報を利用せずに、信頼できるアクセス権設定装置の一手段が自然言語情報を作成する方式を考案する。利用者によ
20 って作成された人工言語情報を含むアクセス要求情報 3 0 3 を基に、人工言語と自然言語を対応させて変換を行い、表示情報作成手段 1 0 9 にて、自然言語形式の表示情報を作成する。

人工言語から自然言語へ翻訳する際の対応を取った変換テーブルの例
25 を図 2 6 に示す。

図 2 6 には、第 2 の実施の形態にて説明した図 8 に示す「アクセス対

象資源」、「アクセス内容」、「条件」などの各人工言語に対応した自然言語が記載されている。例えば、利用者により「対象資源」が「0x0004」で「アクセス内容」が「0x1020」と指定された場合、アクセス権設定装置 100 の表示情報作成手段 109 にて、「ビデオカメラのすべての動作」というように、文字列による自然言語への変換を可能にする。但し、この人工言語はある規約により定められたもので、利用者、管理者、双方で既知であることが前提となる。なお、図 26 には例として自然言語を文字列の形で表しているが、他にも画像、音声などがあり、どの形式を使用してもよい。又、図 26 の変換テーブルを用いた自然言語の作成

5 アルゴリズムは一例であり、作成方式は特に限定しない。

図 27 に、アクセス権設定装置 100、管理者の端末 200、利用者の端末 300 間での動作例を示す。この例では、図 16 に示す管理者の端末 200 を利用するものとして説明する。図 27 は、図 23 に示す第 6 の実施の形態における動作例に、新たな動作 1704～1706 を加えたものであり、残りの 1701～1703 は、1601～1603 に、1706～1717 は、1604～1615 にそれぞれ対応しているため、ここでは説明を省略する。

15

アクセス要求情報受付手段 101 が、暗号化されたアクセス要求情報 303 とそれに付随する CA が発行した証明書、又はデジタル署名を受け付け、アクセス要求情報認証手段 108 へアクセス要求情報 303 の認証を依頼する。復号化に必要な CA、又は利用者の公開鍵は、アクセス要求情報 303 と共に送信されるか、又はネットワーク上のアクセス可能な DB（データベース）から取得できる。該当する公開鍵で暗号化されているアクセス要求情報 303、又は証明書を復号化し、利用者のユーザ認証を行うと共に、公開鍵、秘密鍵を、用いて認証を行う（1704）。認証が通った場合、利用者により人工言語のみで記述されたアク

20

25

セス要求情報 3 0 3 は、表示情報作成手段 1 0 9 にて人工言語を読み取られ、アクセス要求情報 3 0 3 を適切な自然言語へと変換され、結果として人間が理解し易い表示情報が作成される (1 7 0 5)。表示情報作成手段 1 0 9 にて作成された表示情報が、アクセス要求情報転送手段 1 0 5 2 により、管理者の端末 2 0 0 へ転送される (1 7 0 6)。

図 2 8 に、第 7 の実施の形態のアクセス要求情報 3 0 3 の認証手段及びアクセス要求情報 3 0 3 から自然言語を作成する手段を加えたフローチャートを示す。

利用者が作成したアクセス要求情報 3 0 3 を受け付ける (1 8 0 1)。
10 アクセス要求情報 3 0 3 のデジタル署名を参照して信頼できる情報かの認証を行う (1 8 0 2)。認証されない場合は、アクセス要求情報 3 0 3 は設定されず (1 8 0 8)、不許可の結果が利用者へ通知される (1 8 0 9)。認証された場合は、表示情報作成手段 1 0 9 にて、アクセス要求情報の内容を自然言語に変換し、管理者に提示するための表示情報を作成する (1 8 0 3)。以降の 1 8 0 4 ~ 1 8 0 7 は、図 6 に示す 1 1 0 2 ~ 1 1 0 5 と同じフローなので、ここでは説明を省略する。

上述のように構成された本発明の第 7 の実施の形態によれば、デジタル署名を利用した認証の仕組みを利用することで、利用者が信頼でき、更にアクセス要求情報 3 0 3 も信頼できるものか確認を行うことが可能
20 である。特に多種多様なサービスが考えられるホームネットワークでは、ネットワーク上に散在している信頼できないサービスの存在も懸念されるので、このような認証の仕組みを利用することで、不正なサービスの導入を防ぐ効果がある。

又、利用者が用意する管理者へアクセス要求情報の内容を理解してもらうための自然言語情報で、実際の設定内容を誤魔化される恐れがある
25 という課題に対し、信頼できるアクセス権設定装置が、人間が理解でき

る自然言語を用いた表示情報を作成する機能を持つことで、利用者が指定した内容を忠実に管理者へ伝えることができ、利用者による不正なアクセス権の設定を防ぐことが可能となり、セキュリティ向上の効果がある。

5 (実施の形態 8)

図 29 は、本発明第 8 の実施の形態におけるネットワークシステム全体の構成を表すものである。第 8 の実施の形態では、管理者の端末にて行っていた、アクセス要求情報の判定、対象資源の絞込み選択、アクセス要求情報記述の内容の変更を、携帯端末にて行わせることが目的となる。

図 24 に示す第 7 の実施の形態の構成図と異なり、図 29 に示す構成では、アクセス権設定装置 100 内に、管理者がアクセス権の設定を行うために用いる携帯端末 600 と、携帯端末 600 へアクセス要求情報 303 を転送する携帯端末用要求情報転送手段 110 と、携帯端末 600 15 0 にて、アクセス要求情報 303 をアクセス権情報 104 として設定するかの可否判定を行う携帯端末用要求情報判定手段 111 と、携帯端末 600 にて、複数のアクセスの対象となる資源の候補の中から絞込み選択を行う携帯端末用対象資源選択手段 112 と、携帯端末 600 にて、アクセス要求情報 303 に記述された内容の変更を行う携帯端末用要求 20 情報変更手段 113 を備えている。なお、ここで記述している携帯端末 600 とは、人間により比較的自由に持ち運びができ、且つ、ネットワークとの接続手段を備えているものと仮定する。又、管理者の端末 200 及び利用者の端末 300 の構成は変わっていない。

上述の 110、111、112、113、の各手段は、図 16 に示す 25 管理者の端末 200 内にある 202、201、204、205 の各手段を携帯端末用に拡張したもので、目的は同じものと考えてよい。

以上のように構成されたネットワークシステムにおける、アクセス権設定装置及びそのシステムについて、その動作を説明する。

図30に、アクセス権設定装置100、携帯端末600間での動作例を示す。図30では、第7の実施の形態以前のアクセス要求情報303
5 を受け取る処理及び取得する処理と、管理者からの判定結果を受けてのアクセス権の設定処理について、動作が同じであるため省略しており、アクセス権設定装置100と携帯端末600間の動作についてのみ説明する。

アクセス要求情報303を受け付けた、又は取得したアクセス権設定
10 装置100は、携帯端末用要求情報転送手段110により携帯端末600へ転送する。転送された画面の例は図18の通りである(1901)。管理者が携帯端末600の画面上で、図18に示されるような変更ボタンを押すことで、アクセス要求情報303の内容の変更要求を行う(1902)。この要求を受け取った携帯端末用要求情報変更手段113は、
15 管理者の指定した変更画面を携帯端末600へ送信し表示させる(1903)。受け取った管理者は、変更画面にてアクセス要求情報303の記述内容の変更を行う(1904)。管理者が指定した変更内容を受け取った携帯端末用要求情報変更手段113は、その変更内容を反映させた変更結果を携帯端末600へ送信し表示させる(1905)。次に管理者は、
20 アクセス対象資源の候補が複数ある場合に、アクセス対象資源の絞込みのために対象資源の選択要求を行う。この選択は、第4の実施の形態で説明した通り、利用者がアクセス要求情報303のアクセス対象資源の項目に資源の種別を記述した場合に起こり得る処理である(1906)。この要求を受け取った携帯端末用対象資源選択手段112は、管理者の
25 指定した図19に示されるような資源の選択画面を携帯端末600へ送信し表示させる。(1907)。受け取った管理者は、選択画面にてアク

セス対象資源の候補の中から、実際にアクセス権の設定を行う資源の選択を行う(1908)。管理者が指定した選択資源の情報を受け取った携帯端末用対象資源選択手段112は、その選択資源を反映させた選択結果を携帯端末600へ送信し表示させる(1909)。管理者が、アクセス権の設定を許可する判定を行う(1910)。アクセス要求情報303が許可された場合、その情報が携帯端末用要求情報判定手段111まで返る(1911)。なお、1902～1905の変更処理、1906～1909の選択処理及び1910、1911の判定処理の順序は特に限定しない。

10 上述のように構成された本発明の第8の実施の形態によれば、アクセス権設定装置100から携帯端末600へアクセス要求情報303の内容を転送し、アクセス要求情報303の許可判定、アクセス対象資源の選択、アクセス要求情報303に記述された内容の変更といった処理が行えることにより、管理者が外出している場合でも、携帯端末600を
15 持って外出している場合などでも、管理者の端末200で行える処理を携帯端末600で行うことができる。利用者の端末に常にいる必要がなく、又アクセス要求情報303が送信されたり、取得した場合でも、即時に携帯端末まで転送されるので、リアルタイムな設定が可能になる。

20 産業上の利用可能性

以上のように本発明によれば、第1に、利用者による、アクセス権の設定の要求と設定内容の指定ができることにより、ネットワークの知識のない管理者でも簡易にアクセス権の設定が可能になると共に、利用者も希望通りのアクセス権の設定が可能となる。又、ホームネットワーク
25 にサービスを導入するような、頻繁にアクセス権の設定が伴うネットワークでは、アクセス権の設定が簡易なことから特に有効である。

第2に、利用者側からアクセス要求情報を取得することにより、管理者が希望するときに簡易にアクセス権の設定を行うことができ、更に、利用者から一方的にアクセス要求情報を送信されることもなくなるので、不正アクセスの危険度を低くする効果がある。

- 5 第3に、アクセス要求情報に記述された内容をアクセス権情報として設定してもよいかの可否判定を、機械により自動で行えることにより、通常人間が行っていた煩雑な作業を無くすことができ、人間がいない場合でもアクセス権の設定が可能になる効果がある。

- 10 第4に、受け取ったアクセス要求情報から、ユーザIDを発行し、アクセス権情報の一部として登録できることにより、ネットワークのユーザIDを持たずログインできない利用者からも、アクセス要求情報を受け付けることが可能になる。

- 15 第5に、利用者が作成するアクセス要求情報に記述するアクセス対象資源を、抽象化した種別の情報で指定することを可能にしたことにより、利用者はあらかじめ資源の存在や識別子を知っておく必要がなくなり、又管理者は、自分が管理する機密資源の情報を利用者へ知らせる必要がなくなるという効果がある。

- 20 第6に、利用者が種別情報でアクセス要求情報に記述するアクセス対象資源を指定した場合に、複数の対象資源の候補の中から、管理者が自由にアクセスを許可する資源を選択できることにより、管理者の好みに応じて数を絞り込むことができ、余分にアクセス権の設定をしなくてもよいという効果がある。

- 25 第7に、利用者が指定したアクセス要求情報に対し、管理者がその内容の変更ができることにより、一方的に指定されるばかりではなく、管理者の意思を尊重した柔軟な設定や、利用者との交渉をすることで、よりの確な設定が可能という効果がある。

第 8 に、管理者が外部のネットワークに公開した資源の識別子及び種別の情報を、利用者が取得できることにより、資源の情報を知らない利用者でも、アクセス要求情報にアクセス対象資源を記述することができ、アクセス権の設定要求をすることが可能になる。

- 5 第 9 に、利用者が作成したアクセス要求情報の内容を、人間である管理者が理解し易い自然言語へ忠実に変換し、管理者の端末で表示する情報を作成することにより、利用者が管理者に嘘をついて、不正にアクセス権の設定を行わせるのを防ぐ効果がある。

- 10 第 10 に、デジタル署名を利用したアクセス要求情報の認証を行うことにより、不正行為を働こうとしている利用者から、他人のアクセス要求情報を使う成りすましの防止、他人のアクセス要求情報の書き換え防止、並びにアクセス要求情報の信頼性の確認を行うことができる。

- 15 第 11 に、管理者が利用する携帯端末にアクセス要求情報に記述された内容を転送させ、更にアクセス権情報として設定するかの判定も可能にしたことにより、管理者が遠隔地にいる場合や、アクセス要求情報を受け付け、即時に対応したい場合などに効果がある。

第 12 に、第 6 の効果に記載した内容を、管理者が利用する携帯端末でも奏することができる。

- 20 第 13 に、第 7 の効果に記載した内容を、管理者が利用する携帯端末でも奏することができる。

請 求 の 範 囲

1. アクセス権の設定により利用の制限が可能な資源に対し、前記資源の利用を制限するためのアクセス権情報の設定を行うことができるアクセス権設定装置において、

前記資源へのアクセス権設定を要求するための情報が記述されたアクセス要求情報を受け付けるアクセス要求情報受付手段と、

前記アクセス要求情報受付手段により受け付けた前記アクセス要求情報の内容の判定を行うアクセス要求情報判定手段と、

前記アクセス要求情報判定手段により判定した前記アクセス要求情報の内容を、前記アクセス権情報として設定を行うアクセス要求情報設定手段を備えたことを特徴とするアクセス権設定装置。

2. アクセス権の設定により利用の制限が可能な資源に対し、前記資源の利用を制限するためのアクセス権情報の設定を行うことができるアクセス権設定装置において、

前記資源へのアクセス権設定を要求するための情報が記述されたアクセス要求情報の取得を依頼するアクセス要求情報取得依頼手段と、

前記アクセス要求情報取得依頼手段により指定された前記アクセス要求情報の取得を行うアクセス要求情報受付手段と、

前記アクセス要求情報受付手段により取得した前記アクセス要求情報の内容の可否判定を行うアクセス要求情報判定手段と、

前記アクセス要求情報判定手段により判定した前記アクセス要求情報の内容を、前記アクセス権情報として設定を行うアクセス要求情報設定手段を備えたことを特徴とするアクセス権設定装置。

3. アクセス権の設定により利用の制限が可能な資源に対し、前記資源の利用を制限するためのアクセス権情報の設定を行うことができるアクセス権設定装置であって、

前記資源へのアクセス権設定を要求するための情報が記述されたアクセス要求情報を受け付けるアクセス要求情報受付手段と、

前記アクセス要求情報受付手段により受け付けた前記アクセス要求情報の内容の判定を行うアクセス要求情報判定手段と、

前記アクセス要求情報判定手段により判定した前記アクセス要求情報の内容を、前記アクセス権情報として設定を行うアクセス要求情報設定手段を備えたアクセス権設定装置とネットワークにて接続された管理者端末において、

前記資源へのアクセス権設定を要求するための情報が記述されたアクセス要求情報の取得を依頼するアクセス要求情報取得依頼手段と、

前記アクセス権設定装置より前記アクセス要求情報を受け取り、前記アクセス要求情報の内容の可否判定を行うアクセス要求情報判定手段と、

自動的に可否判定を行うアクセス要求情報自動判定手段を備えたことを特徴とする管理者端末。

4. アクセス権の設定により利用の制限が可能な資源に対し、前記資源の利用を制限するためのアクセス権情報の設定を行うことができるアクセス権設定装置であって、

前記資源へのアクセス権設定を要求するための情報が記述されたアクセス要求情報の取得を依頼するアクセス要求情報取得依頼手段と、

前記アクセス要求情報取得依頼手段により指定された前記アクセス要求情報の取得を行うアクセス要求情報受付手段と、

前記アクセス要求情報受付手段により取得した前記アクセス要求情報

の内容の可否判定を行うアクセス要求情報判定手段と、

前記アクセス要求情報判定手段により判定した前記アクセス要求情報の内容を、前記アクセス権情報として設定を行うアクセス要求情報設定手段を備えたアクセス権設定装置とネットワークにて接続された管理者端末において、

前記資源へのアクセス権設定を要求するための情報が記述されたアクセス要求情報の取得を依頼するアクセス要求情報取得依頼手段と、

前記アクセス権設定装置より前記アクセス要求情報を受け取り、前記アクセス要求情報の内容の可否判定を行うアクセス要求情報判定手段と、

自動的に可否判定を行うアクセス要求情報自動判定手段を備えたことを特徴とする管理者端末。

5. 請求項 1 又は 2 に記載のアクセス権設定装置において、

前記資源へアクセスするための前記アクセス権設定装置への接続ができない利用者向けに、前記接続を可能にするためのユーザ認証を行うのに必要な利用者を一意に特定する識別子を発行し、前記アクセス権情報の一部として登録する利用者識別子登録手段を備えたことを特徴とするアクセス権設定装置。

6. 請求項 1、2 及び 5 のいずれか 1 つに記載のアクセス権設定装置において、

前記アクセス要求情報に記述するアクセス権設定の対象となる前記資源の指定について、前記資源を一意に特定する識別子ではなく、前記資源の種別の識別子で指定された前記アクセス要求情報を受け付けることが可能なアクセス要求情報受付手段を備えたことを特徴とするアクセス権設定装置。

7. 請求項 3 又は 4 記載の管理者端末において、

前記アクセス要求情報に記述するアクセス権設定の対象となる前記資源を、前記アクセス要求情報に記述するアクセス権設定の対象となる前記資源の指定について、前記資源を一意に特定する識別子ではなく、前記資源の種別の識別子にて指定したときに、該当する前記資源が複数存在する場合、前記管理者が前記複数の資源の中から利用の対象となる前記資源を選択できるアクセス対象資源選択手段を備えたことを特徴とする管理者端末。

8. 請求項 3、4 及び 7 のいずれか 1 つに記載の管理者端末において、

前記アクセス権設定装置より受け取った前記アクセス要求情報に記述された内容の変更が可能な、アクセス要求情報変更手段を備えたことを特徴とする管理者端末。

9. 請求項 1、2、5 及び 6 のいずれか 1 つに記載のアクセス権設定装置において、

前記アクセス要求情報に記述するアクセス権設定の対象となる前記資源の指定について、前記資源を一意に特定する識別子ではなく、前記資源の種別の識別子の情報の内、前記資源のアクセス元に対して公開する情報として記憶可能な公開資源情報記憶装置を備えたことを特徴とするアクセス権設定装置。

10. 請求項 1、2、5、6 及び 9 のいずれか 1 つに記載のアクセス権設定装置において、

前記アクセス要求情報を正確に前記管理者へ通知するために、前記アクセス要求情報に記述された内容を、視覚的に理解し易い自然言語へ変換することが可能な表示情報作成手段を備えたことを特徴とするアクセス権設定装置。

11. 請求項1、2、5、6、9及び10のいずれか1つに記載のアクセス権設定装置において、

前記アクセス要求情報が、改ざん、又は成りすましに代表される不正行為によって作成されていないこと確認するため、前記アクセス要求情報の認証を行うアクセス要求情報認証手段を備えたことを特徴とするアクセス権設定装置。

12. 請求項1、2、5、6、9、10及び11のいずれか1つに記載のアクセス権設定装置において、

前記アクセス要求情報に記述された内容を遠隔地で把握するために携帯端末へ転送する携帯端末用要求情報転送手段と、

前記アクセス要求情報の可否判定を前記携帯端末から行うための携帯端末用要求情報判定手段を備えたことを特徴とするアクセス権設定装置。

13. 請求項12に記載のアクセス権設定装置において、

前記アクセス要求情報に記述するアクセス権設定の対象となる前記資源を、前記アクセス要求情報に記述するアクセス権設定の対象となる前記資源の指定について、前記資源を一意に特定する識別子ではなく、前記資源の種別の識別子にて指定したときに、該当する前記資源が複数存在する場合、前記管理者が前記複数の資源の中から利用の対象となる前記資源を選択できるアクセス対象資源選択手段にて行う前記アクセス対

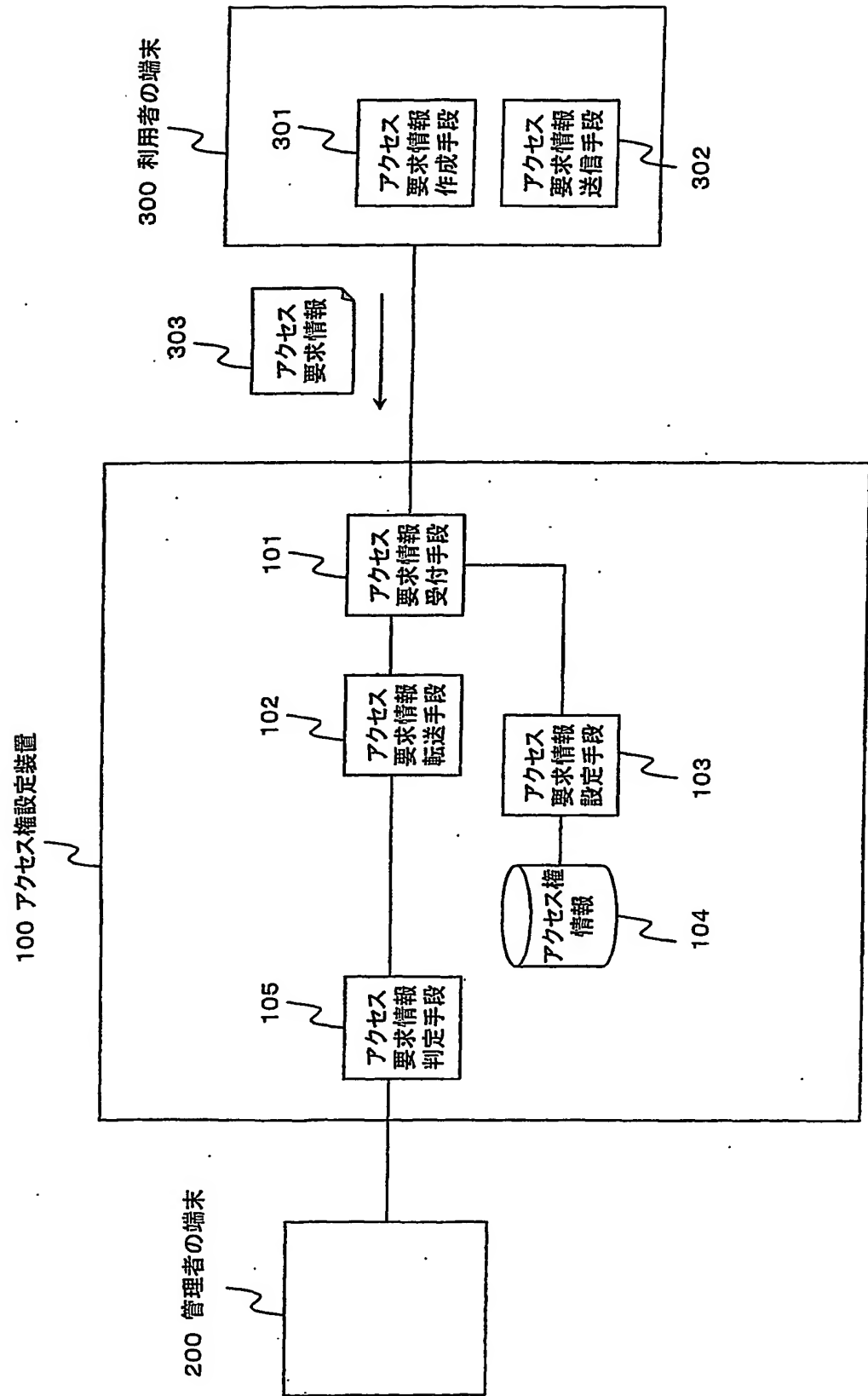
象の資源の選択を、前記携帯端末から行うための携帯端末用対象資源選択手段を備えたことを特徴とするアクセス権設定装置。

14. 請求項12又は13に記載のアクセス権設定装置において、
前記アクセス要求情報に記述された内容の変更を、前記携帯端末から
行うための携帯端末用要求情報変更手段を備えたことを特徴とするア
クセス権設定装置。

THIS PAGE BLANK (USPTO)

1/27

図1



THIS PAGE BLANK (USPTO)

図 2

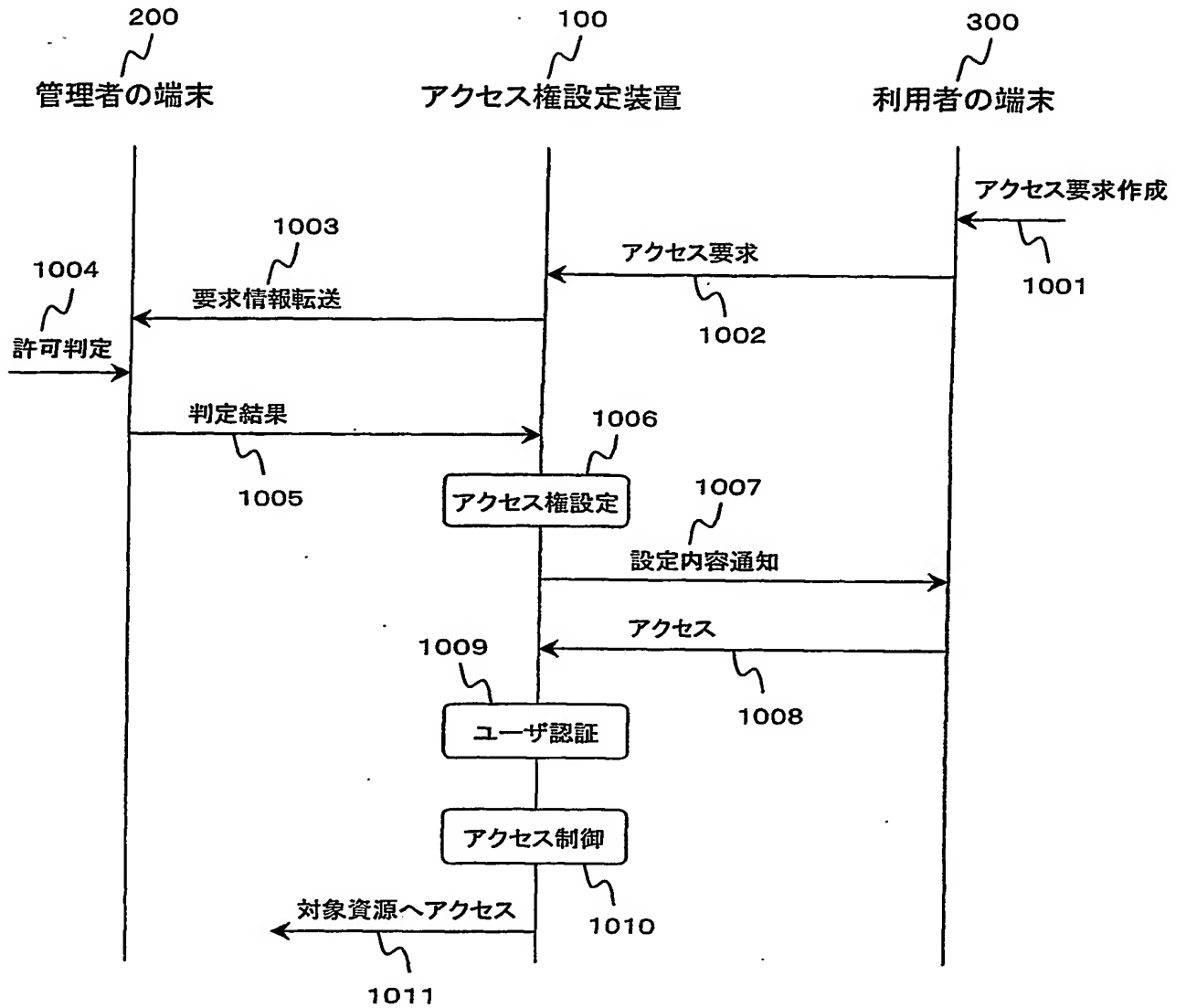
アクセス要求情報の例

利用者 :	利用者 A
利用端末 :	111. 222. 111. 222
期間 :	2000/1/25 ~ 2000/2/29
アクセス対象資源 :	ファイルB
アクセス内容 :	読み出し、書き込み

THIS PAGE BLANK (USPTO)

3/27

図 3



THIS PAGE BLANK (USPTO)

図 4

判定画面の例

「利用者A」	詳細
さんから	
「ファイルB」への「読み出し権、書き込み権」 に対するアクセスの要求がきています	
2000年1月1日から2000年2月29日まで	
許可	不許可

図 5

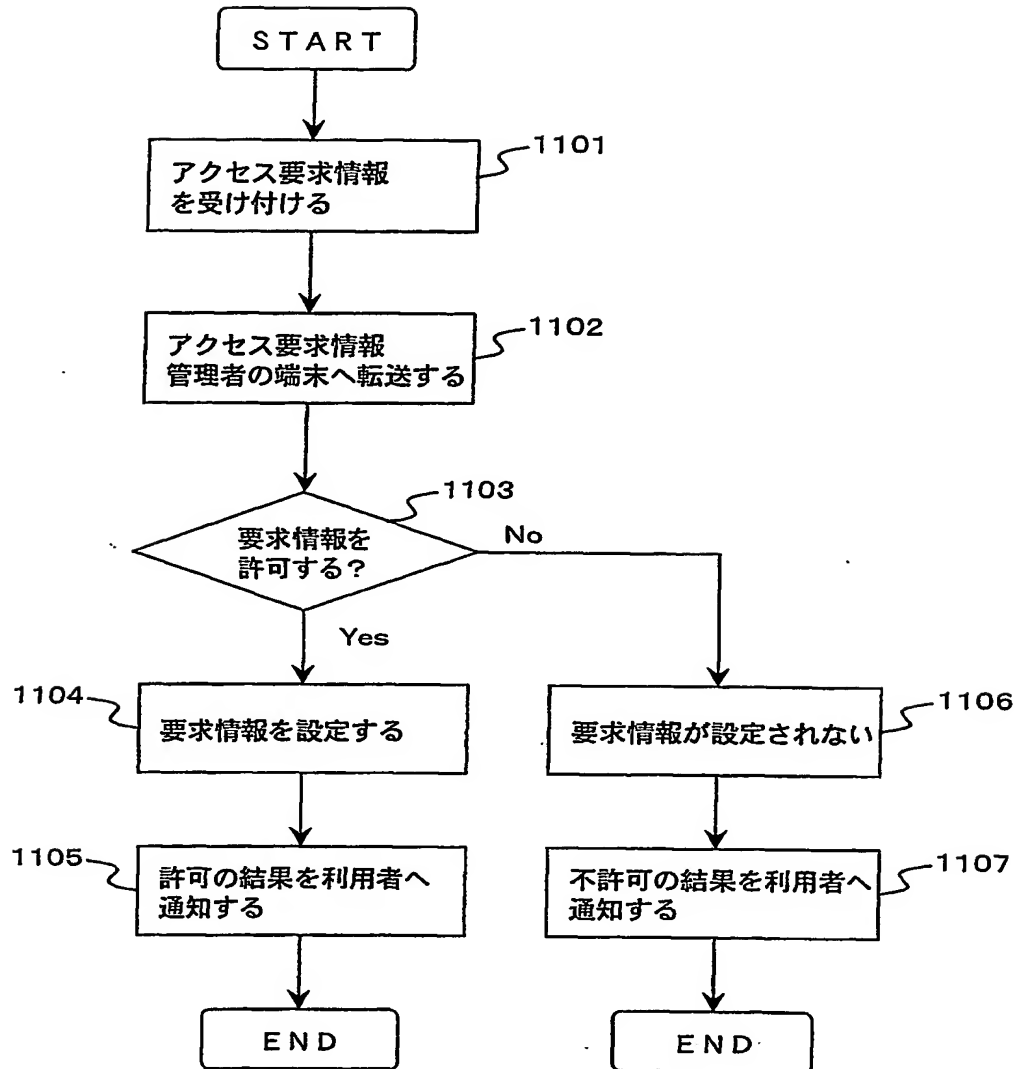
利用者への通知画面の例

「利用者A」様
2000年1月1日から2000年2月29日までの期間、 「ファイルB」への「読み出し権、書き込み権」 を設定いたしました。

THIS PAGE BLANK (USPTO)

5/27

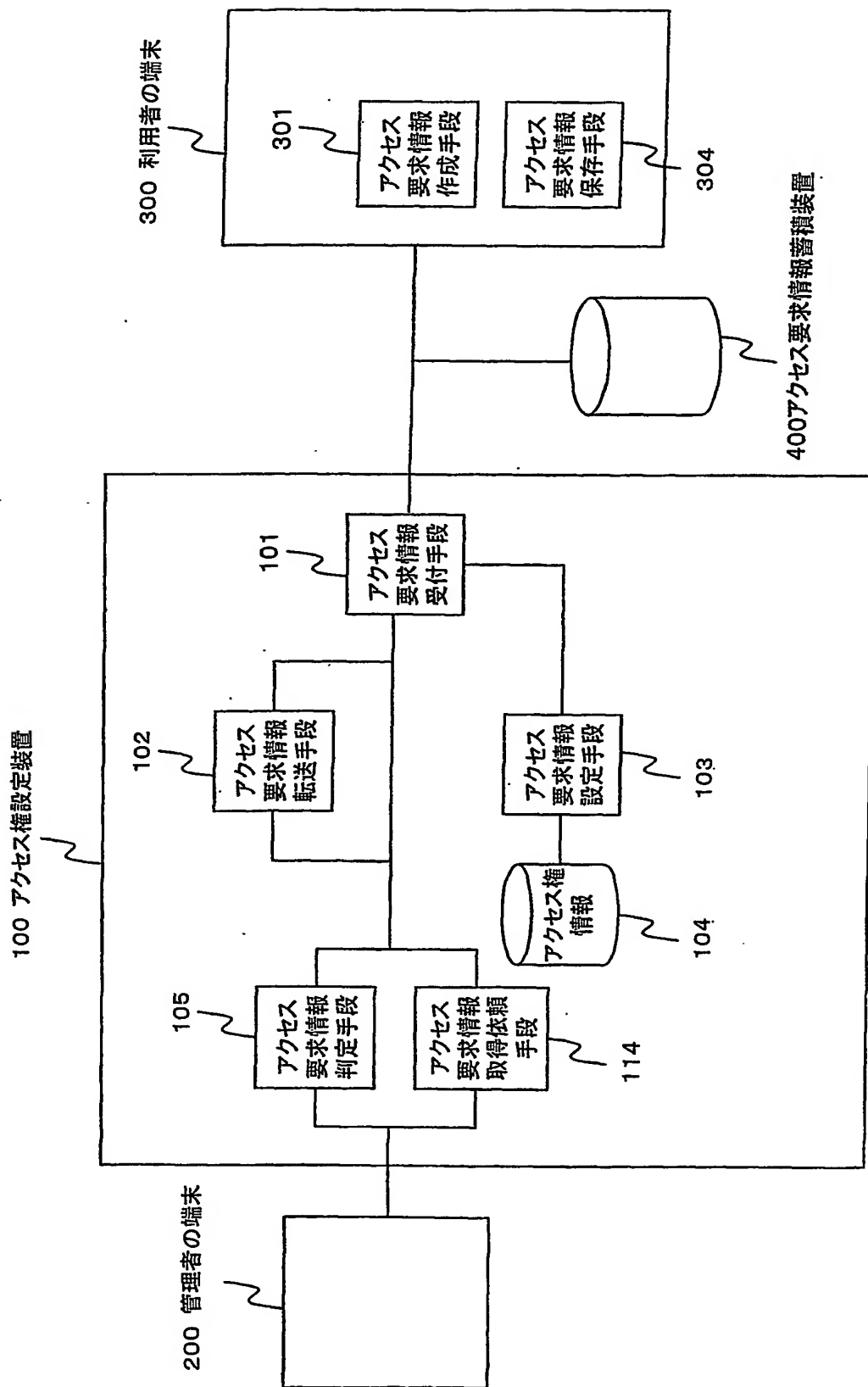
図 6



THIS PAGE BLANK (USPTO)

6/27

図7



THIS PAGE BLANK (USPTO)

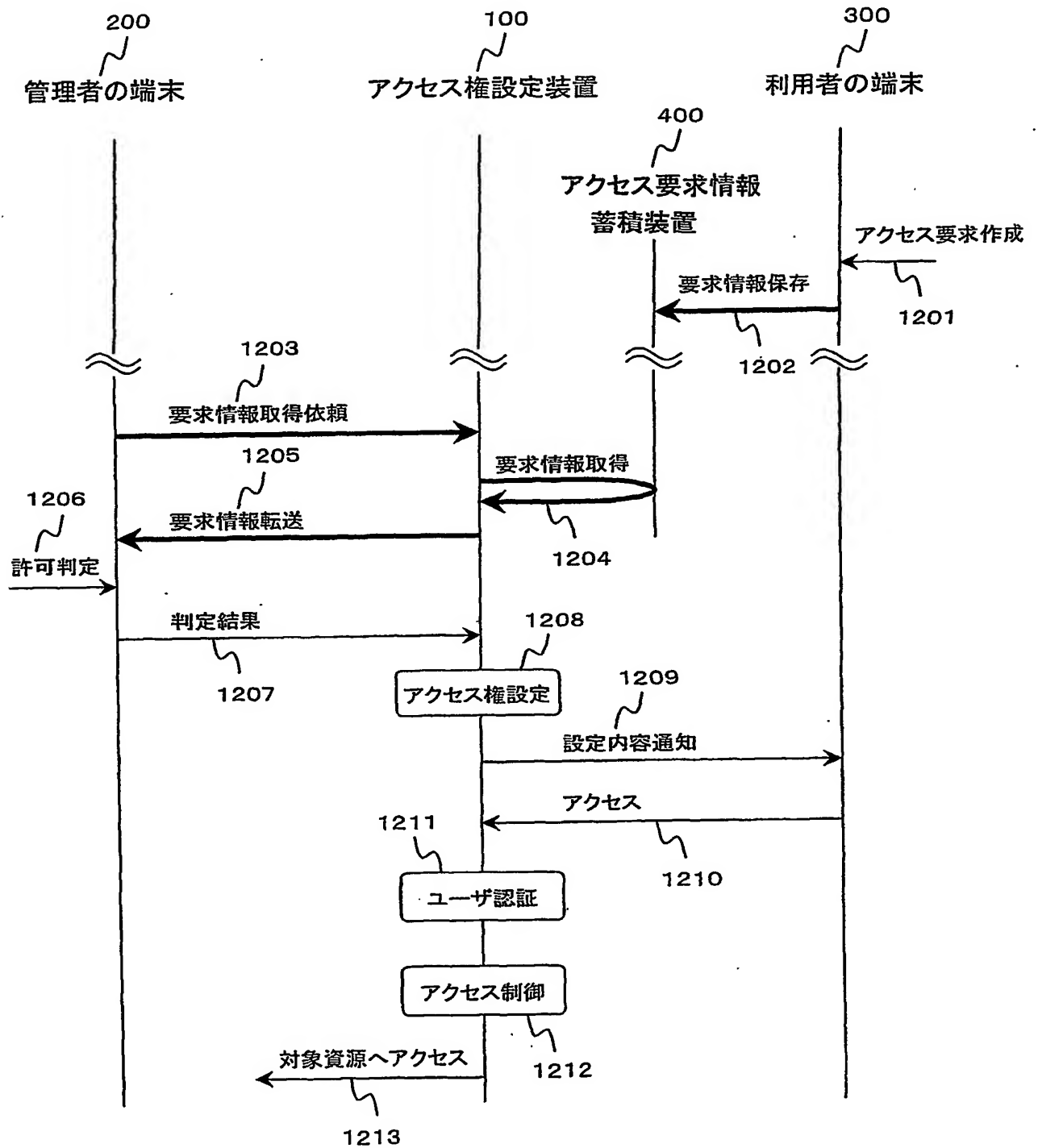
アクセス要求情報の例

利用者 :	警備会社 A
	遠隔監視サービス
属性 :	セキュリティ
利用端末 :	123. 456. 789. 123
期間 :	2000/1/1 ~ 2000/2/29
アクセス対象資源 :	ビデオカメラ B
アクセス内容 :	映像取得
条件 :	警報センサ反応時

THIS PAGE BLANK (USPTO)

8/27

図 9



THIS PAGE BLANK (USPTO)

9/27

図 10

サービス一覧画面の例

■ サービス一覧

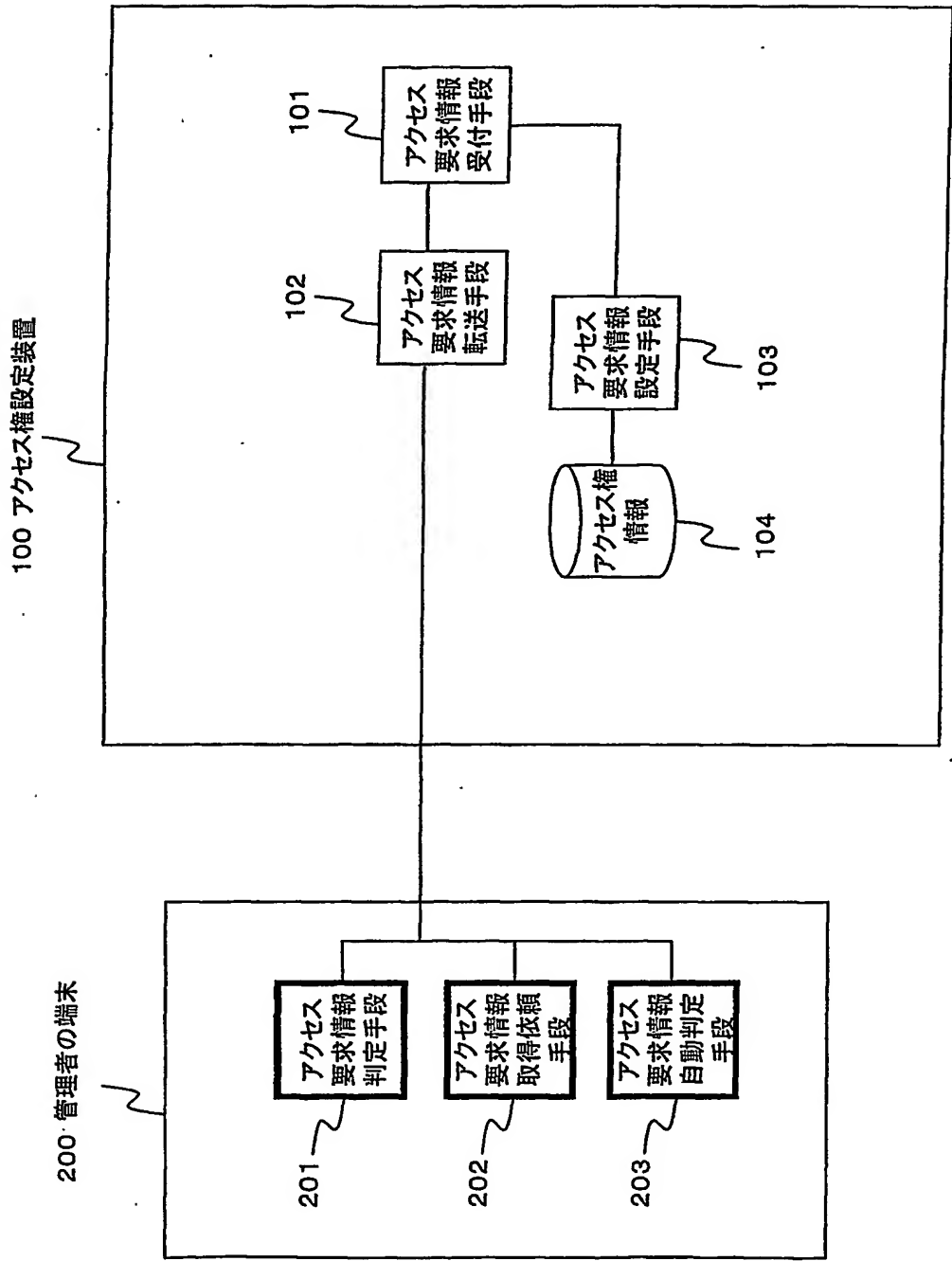
以下のサービスを受けることができます。

1. 遠隔監視サービス
2. 遠隔医療サービス
3. 遠隔機器メンテナンスサービス

THIS PAGE BLANK (USPTO)

10/27

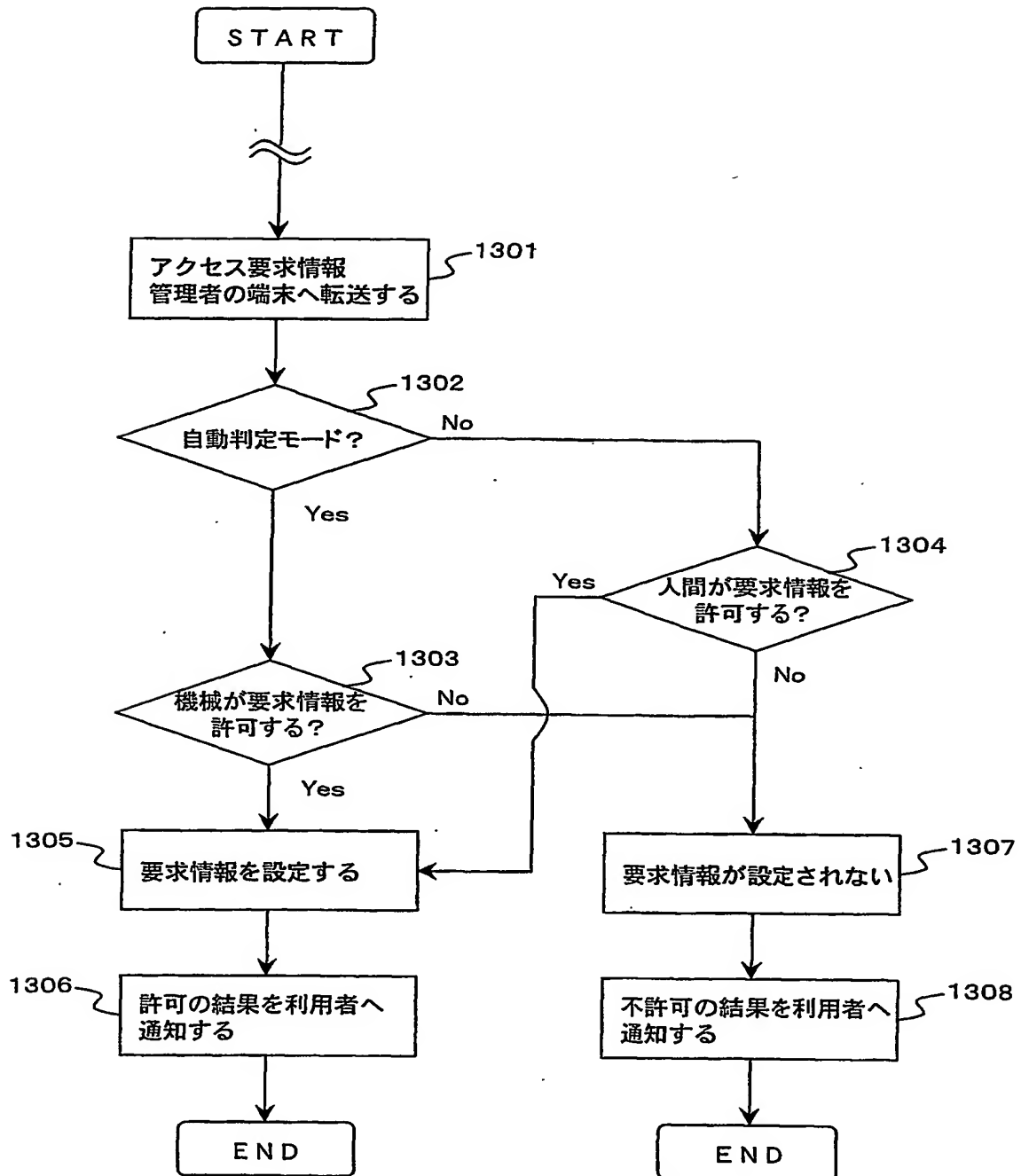
図 11



THIS PAGE BLANK (USPTO)

11/27

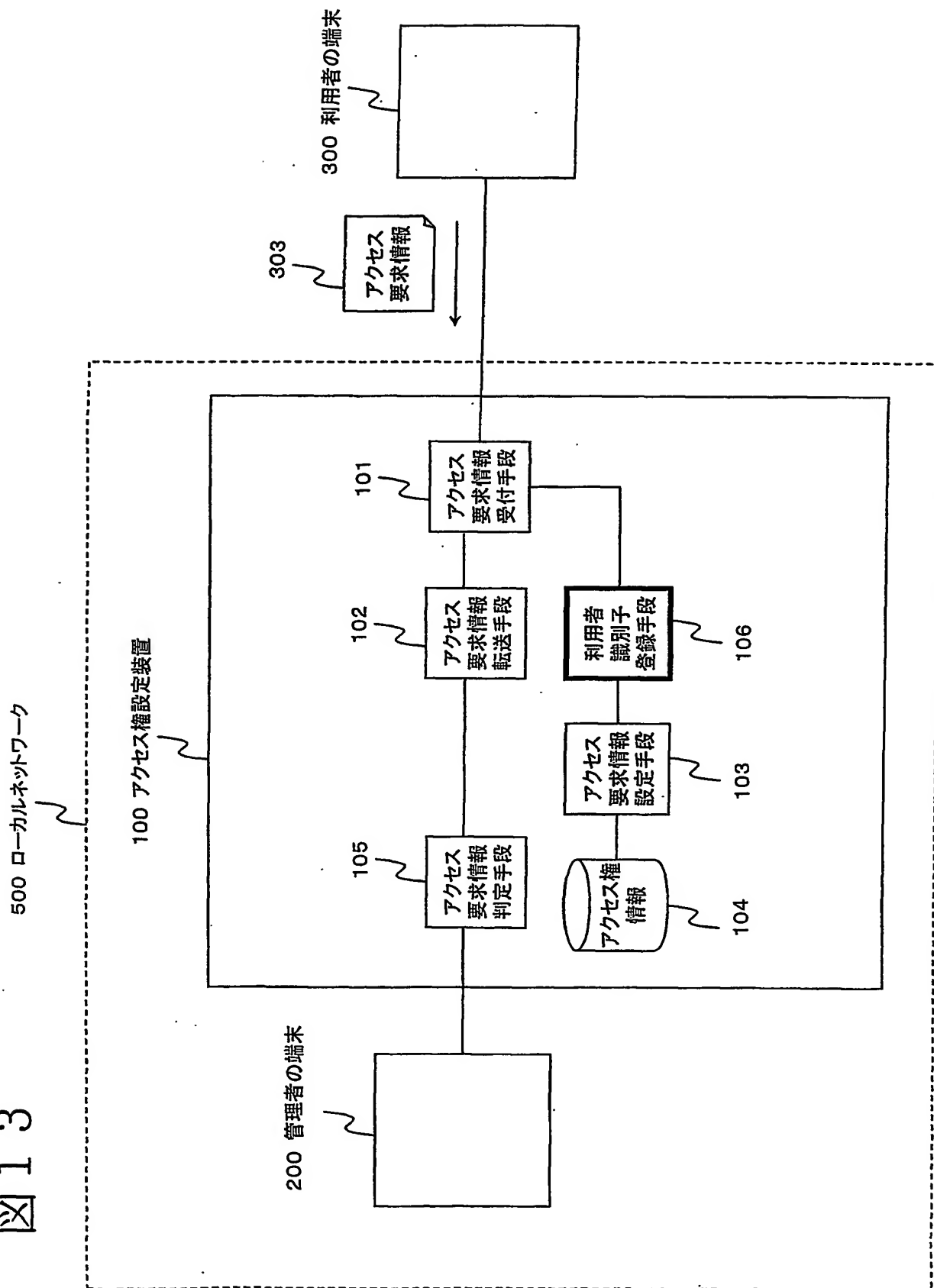
図 1 2



THIS PAGE BLANK (USPTO)

12/27

図 13



THIS PAGE BLANK (USPTO)

図 1 4

アクセス対象資源の種別情報

アクセス対象資源 : ビデオカメラB



抽象化

アクセス対象資源 : ビデオカメラ全部

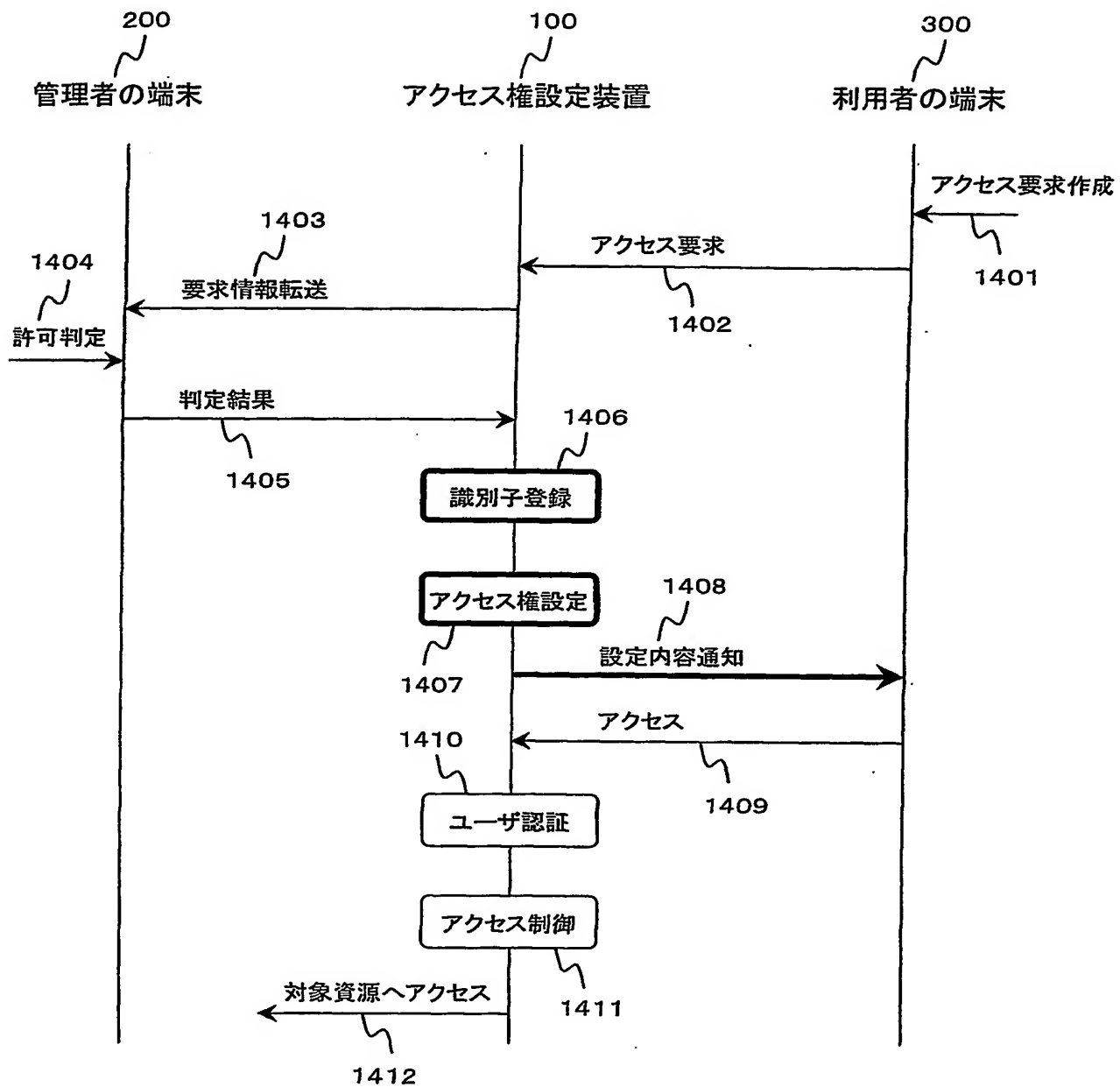
アクセス対象資源 : ビデオカメラ1台

アクセス対象資源 : ○○○製のビデオカメラ

THIS PAGE BLANK (USPTO)

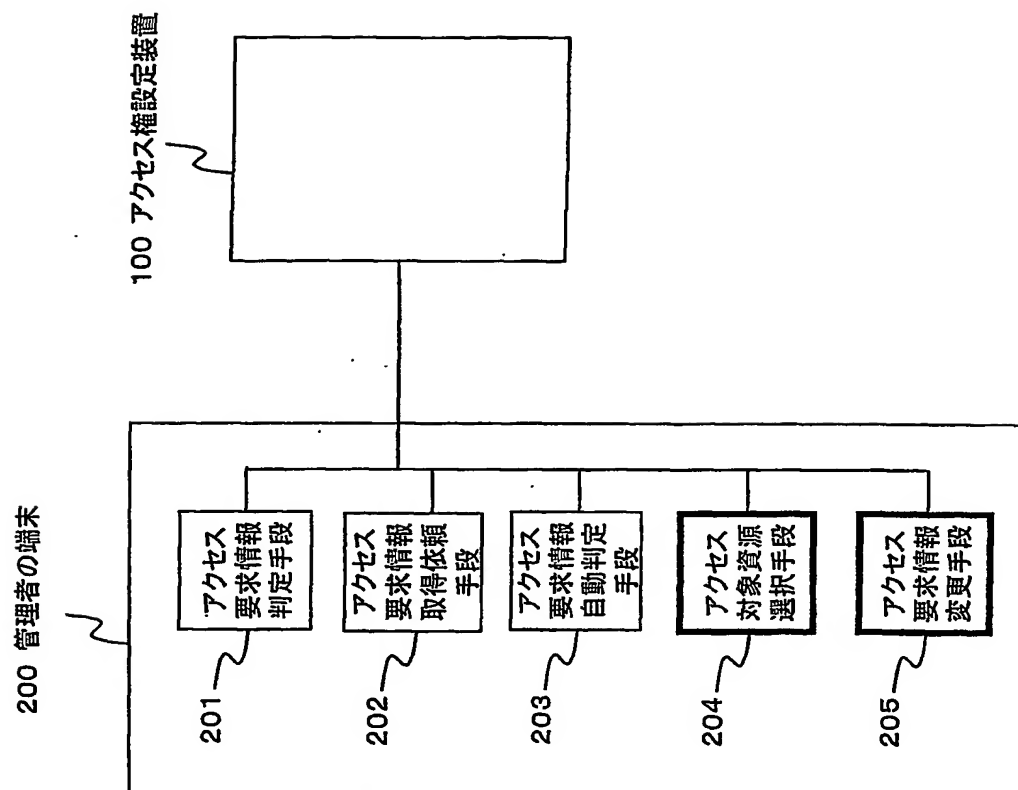
14/27

図 15



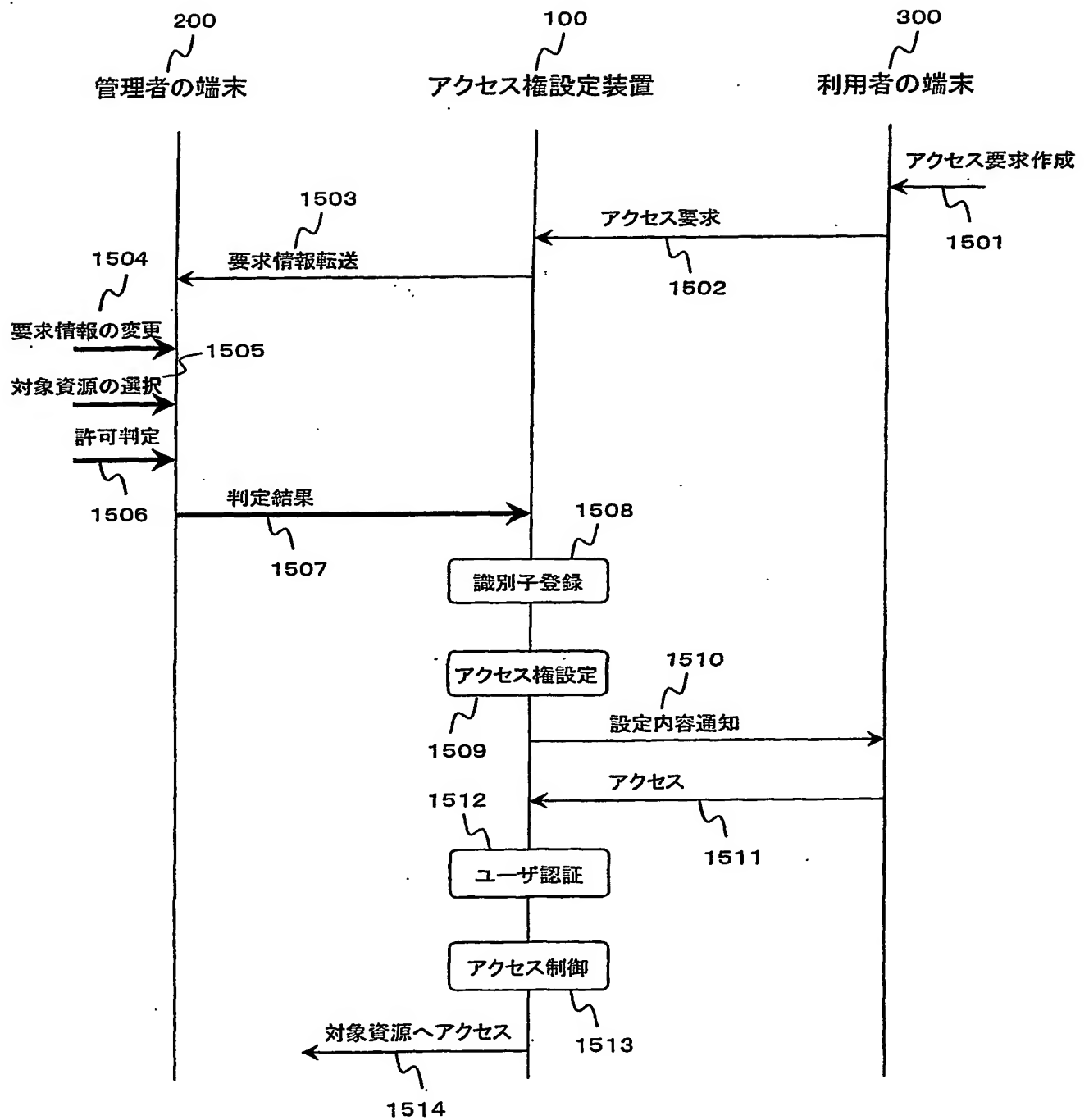
THIS PAGE BLANK (USPTO)

図 16



THIS PAGE BLANK (USPTO)

図 17



THIS PAGE BLANK (USPTO)

図 1 8

内容表示画面の例

「利用者 A」

詳細

さんから、アクセス権設定の要求がきています。

変更

「ビデオカメラ B」への

変更

「映像取得」

変更

2000年1月1日から2000年2月29日まで

変更

「警報センサ反応時」に行います。

許可

不許可


図 1 9


選択画面の例


選択

「ビデオカメラ 1 台」

どのビデオカメラを選択しますか？
(3台の選択可能なビデオカメラがあります。)


[部屋用]


[玄関用]

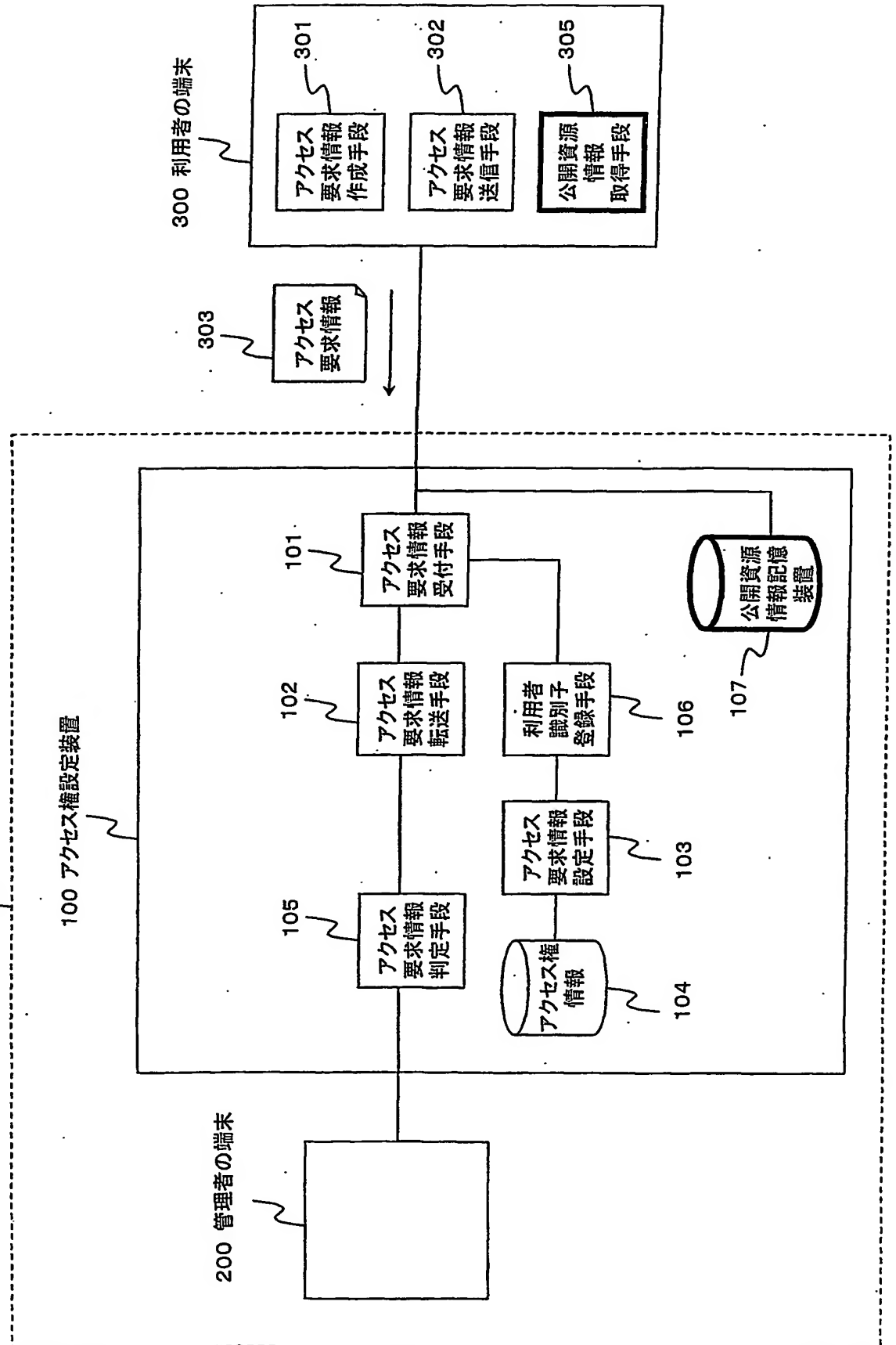

[庭用]

THIS PAGE BLANK (USPTO)

18/27

図 20

500 ローカルネットワーク



THIS PAGE BLANK (USPTO)

図 2 1

公開資源情報の例

[対象資源]	[アクセス内容]
ビデオカメラA	映像取得
ビデオカメラB	ALL
デジタルテレビC	ALL

図 2 2

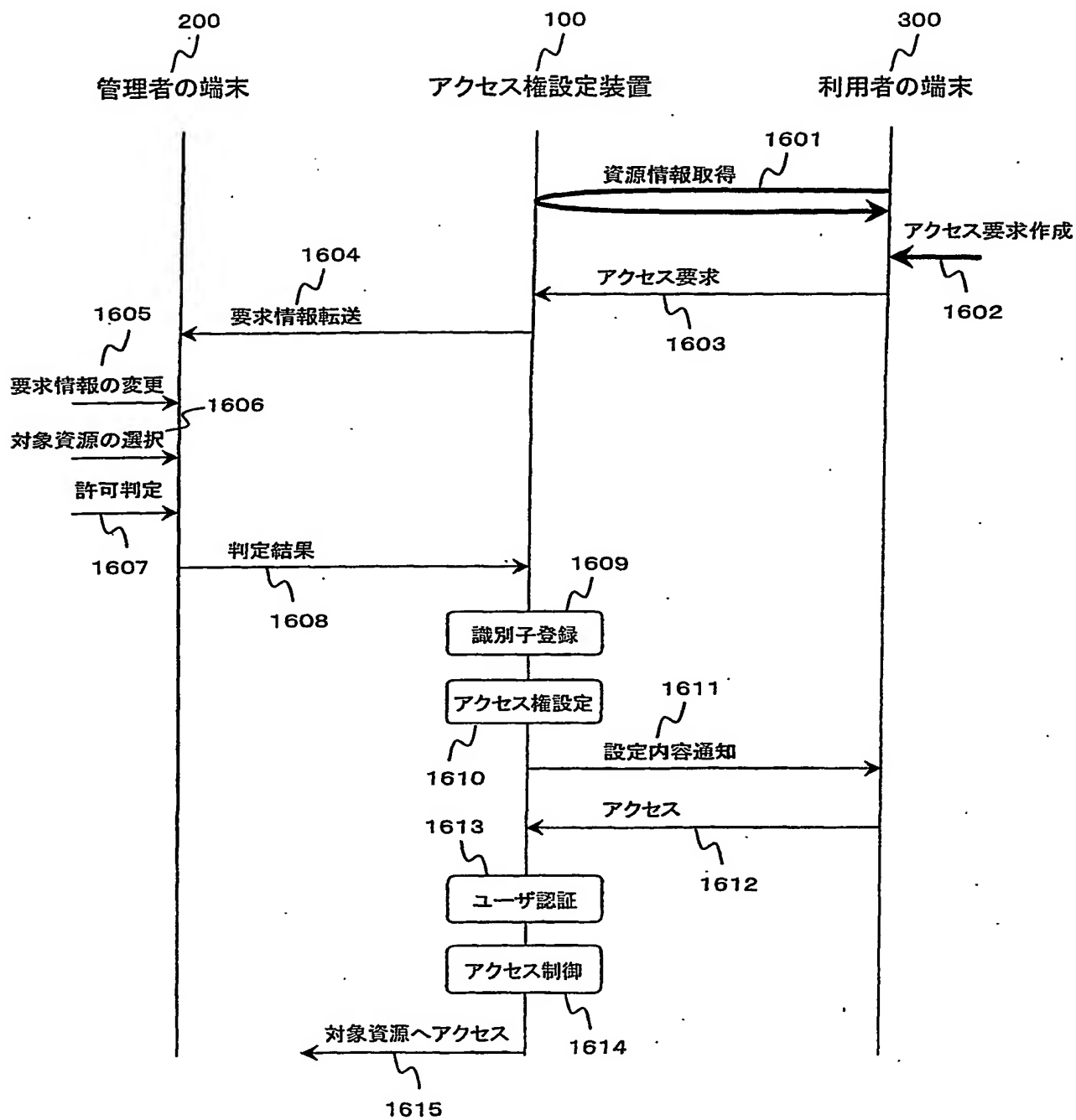
公開資源情報の例(種別情報)

[対象資源]
ビデオカメラ
デジタルテレビ

THIS PAGE BLANK (USPTO)

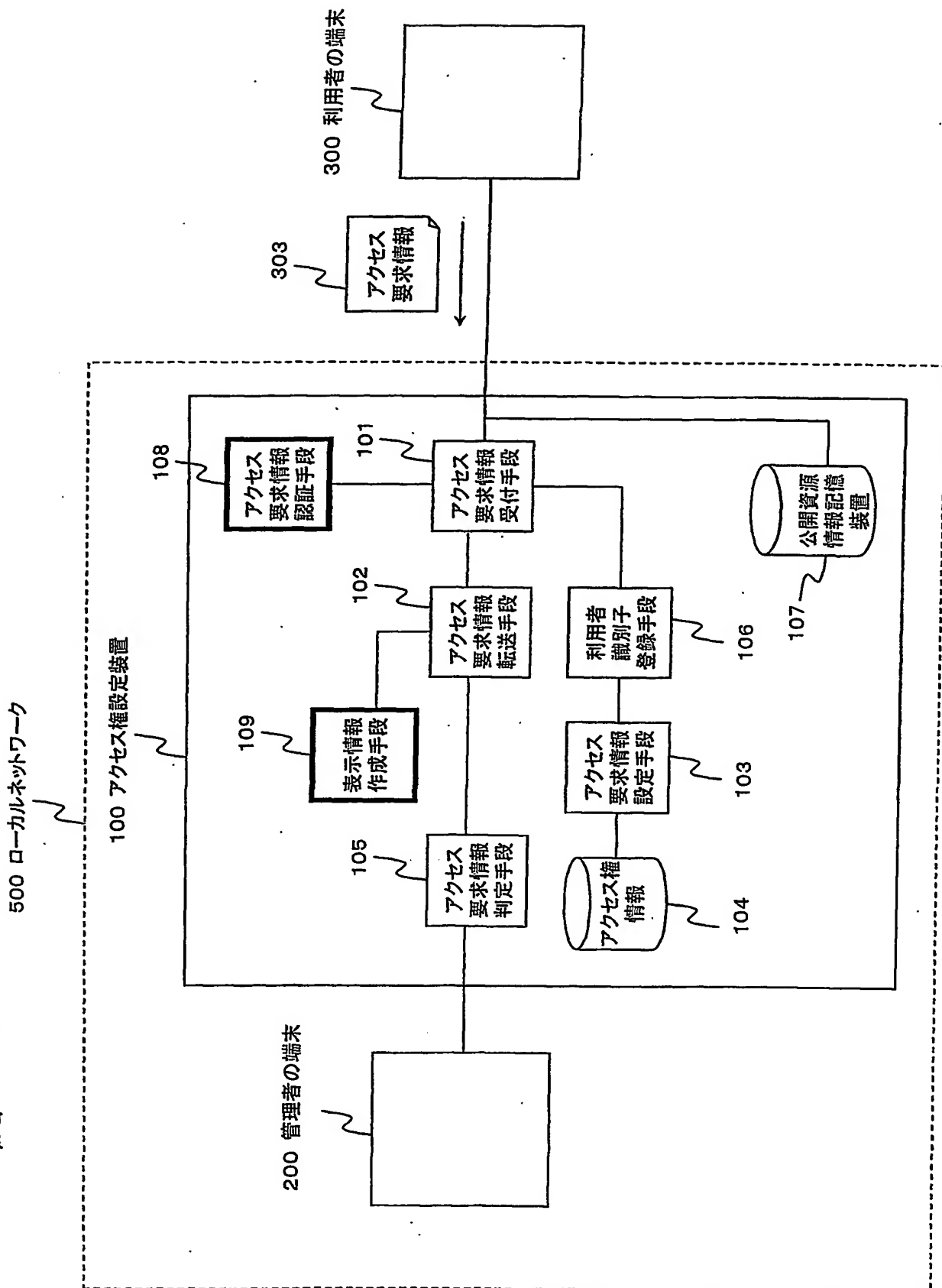
20/27

図 2 3



THIS PAGE BLANK (USPTO)

図 24



THIS PAGE BLANK (USPTO)

図 2 5

アクセス要求情報(不正情報)の例

[人工言語]

<アクセス要求情報>

<利用者>

<会社名>警備会社A</会社名>

<サービス名>遠隔監視サービス</サービス名>

</利用者>

<期間>

<開始>20000101</開始>

<終了>20000229</終了>

</期間>

<アクセス対象資源>0x0004</アクセス対象資源>

<アクセス内容>0x1020</アクセス内容>

.....

</アクセス要求情報>

[自然言語]

警備会社Aの遠隔監視サービスへお申し込み
いただき、誠にありがとうございます。

「1999年12月1日から2000年5月31日まで」の期間、
「ビデオカメラ」の「映像取得」を行いますので、
アクセス権の設定をお願いします。

THIS PAGE BLANK (USPTO)

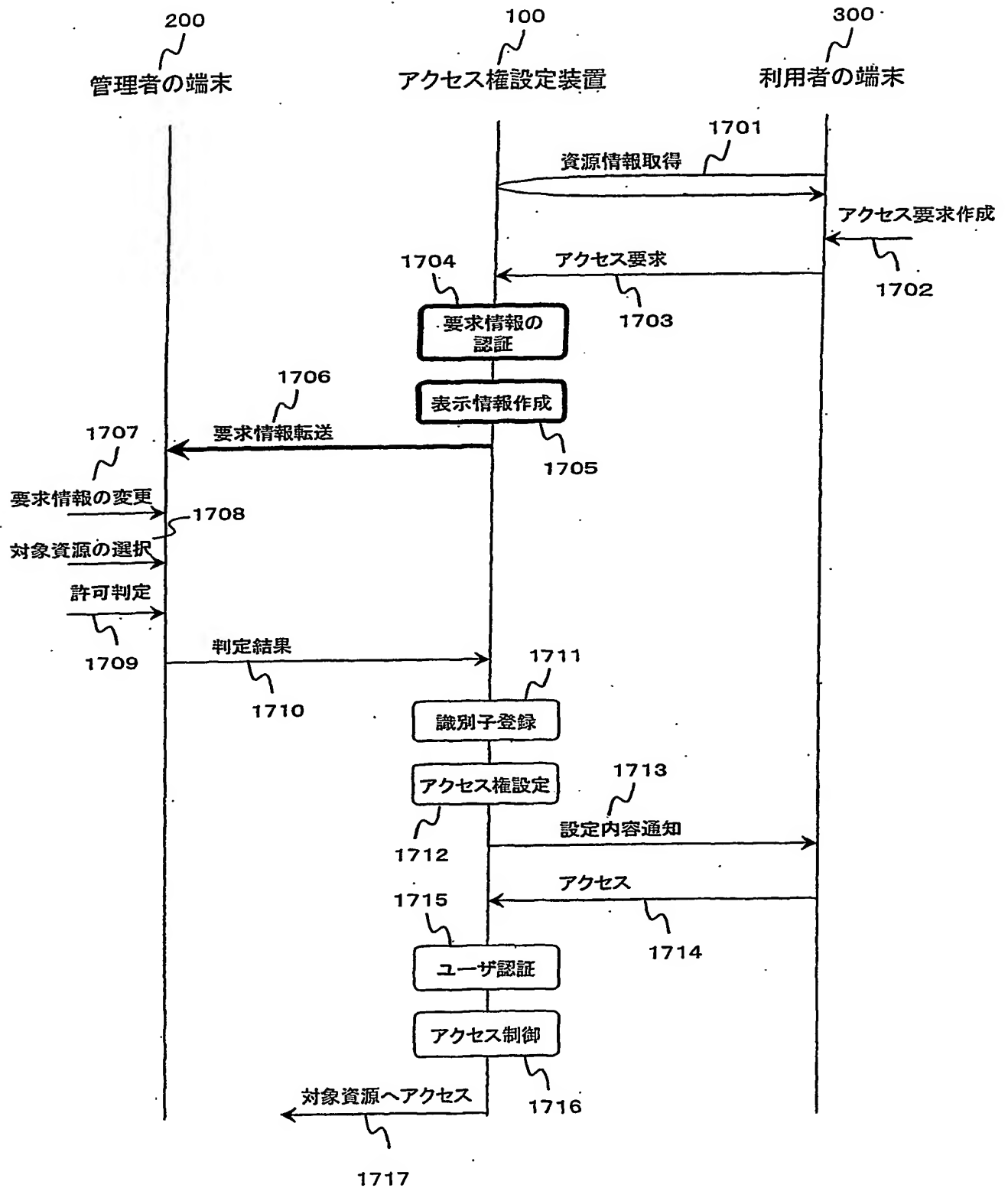
図 2 6

変換テーブルの例

[人工言語]	[自然言語]
・対象資源	
0x0004	ビデオカメラ
0x0010	デジタルテレビ
.....
・アクセス内容	
0x1008	映像取得
0x1020	すべての動作
.....

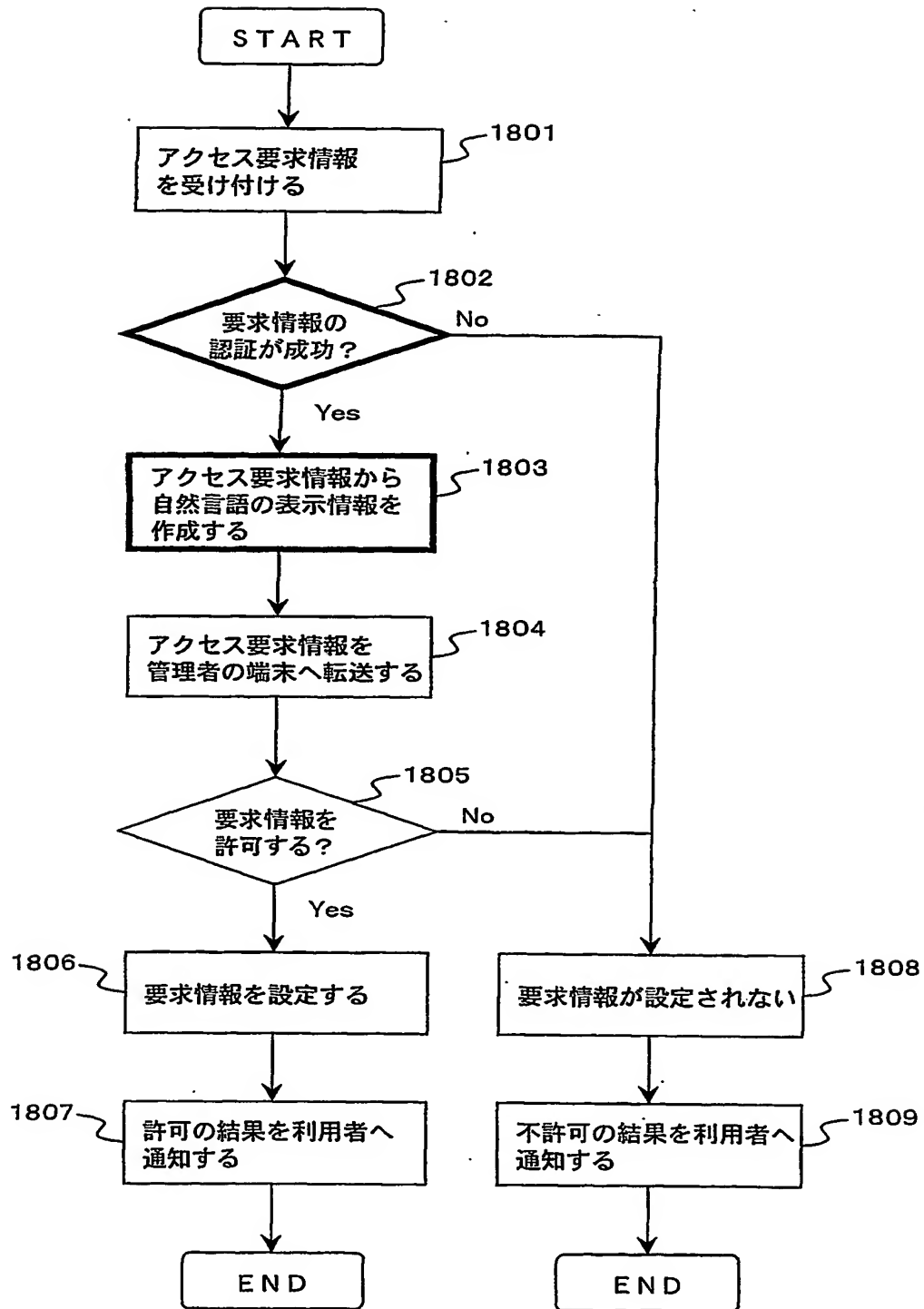
THIS PAGE BLANK (USPTO)

図 27



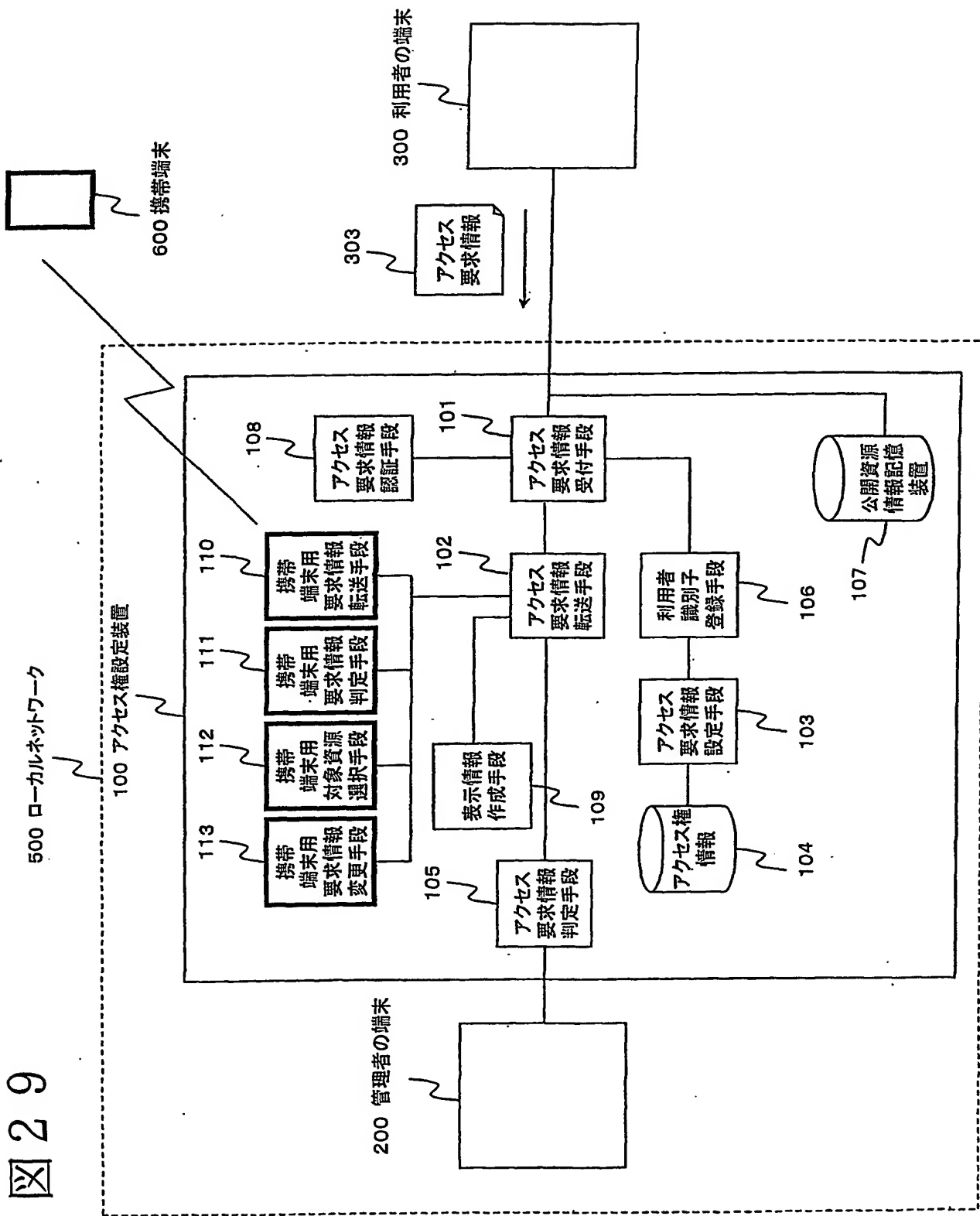
THIS PAGE BLANK (USPTO)

図 28



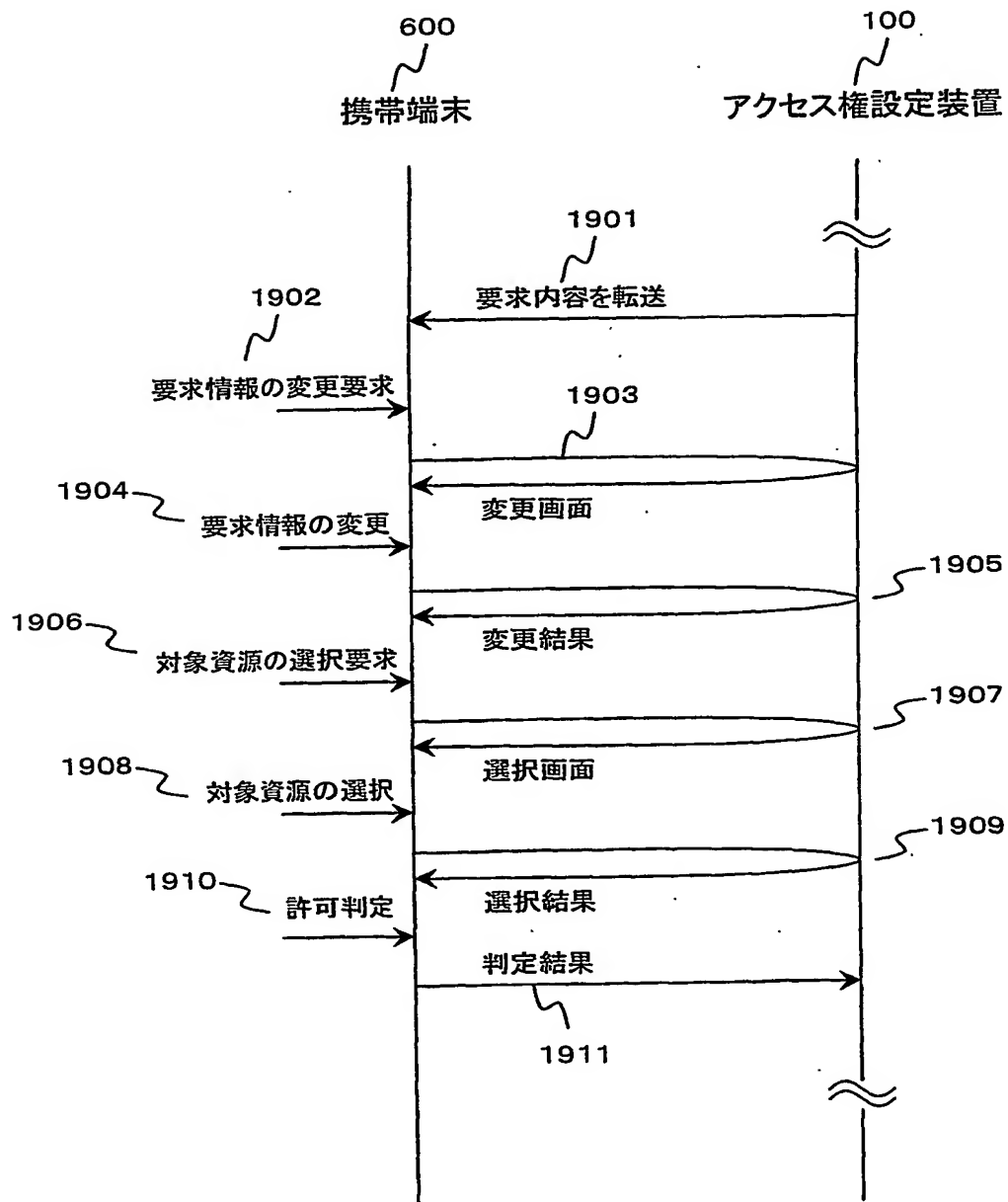
THIS PAGE BLANK (USPTO)

図 29



THIS PAGE BLANK (USPTO)

図 30



THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/03515

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.⁷ G06F12/00, G06F13/00, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.⁷ G06F12/00, G06F13/00, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho	1971-2001	Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"Muryou Build-kei Site de Homepage wo tsukurou", INTERNET magazine, August, 1999, No. 55, pp.294-301	1-14
Y	Oosaka Daigaku Joho Shori Kyouiku Kenkyukai ed. NeXt User Guide Book, 1 st printing, Askii Shuppankyoku, 20 June, 1992 (20.06.92), pp. 33-52	1-14
A	Fumi SAKAMOTO, UNIX e no Shoutai, UNIX MAGAZINE, May, 1991, Vol.6, No.5, pp. 151-164	1-14



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
17 July, 2001 (17.07.01)

Date of mailing of the international search report
21 August, 2001 (21.08.01)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

THIS PAGE BLANK (USPTO)

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/00, G06F13/00, G06F15/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/00, G06F13/00, G06F15/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996

日本国公開実用新案公報 1971-2001

日本国登録実用新案公報 1994-2001

日本国実用新案登録公報 1996-2001

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	無料ビルド系サイトでホームページを作ろう, INTERNET magazine, 8月.1999, 第55号, p. 294 - 301	1 - 14
Y	大阪大学情報処理教育研究会 編, NeXT ユーザーガイドブック 第1版, アスキー出版局, 20.6月.1992 (20.06.92), p. 33 - 52	1 - 14
A	坂本 文, UNIXへの招待, UNIX MAGAZINE, 5月.1991, 第6巻, 第5号, p. 151 - 164	1 - 14

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

17.07.01

国際調査報告の発送日

21.08.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

原 秀人

5 N

9 6 4 4

電話番号 03-3581-1101 内線 3585

THIS PAGE BLANK (USPTO)

国際調査報告

(法8条、法施行規則第40、41条)
[PCT18条、PCT規則43、44]

出願人又は代理人 の書類記号 P62-0103	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220)及び下記5を参照すること。		
国際出願番号 PCT/JPO1/03515	国際出願日 (日.月.年) 24.04.01	優先日 (日.月.年) 24.04.00	
出願人(氏名又は名称) 松下電器産業株式会社			

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 2 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

- a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。
- b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

3. ☐ 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。
☐ 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、
第 1 図とする。 ☒ 出願人が示したとおりである。 ☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

THIS PAGE BLANK (USPTO)

A. 発明の属する分野の分類 (国際特許分類 (IPC))
Int. Cl⁷ G06F12/00, G06F13/00, G06F15/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))
Int. Cl⁷ G06F12/00, G06F13/00, G06F15/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996
日本国公開実用新案公報 1971-2001
日本国登録実用新案公報 1994-2001
日本国実用新案登録公報 1996-2001

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	無料ビルド系サイトでホームページを作ろう, INTERNET magazine, 8月.1999, 第55号, p. 294 - 301	1 - 14
Y	大阪大学情報処理教育研究会 編, NeXT ユーザーガイドブック 第1版, アスキー出版局, 20.6月.1992 (20.06.92), p. 33 - 52	1 - 14
A	坂本 文, UNIXへの招待, UNIX MAGAZINE, 5月.1991, 第6巻, 第5号, p. 151 - 164	1 - 14

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

17.07.01

国際調査報告の発送日

21.08.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
郵便番号 100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

原 秀人

5 N

9 6 4 4

電話番号 03-3581-1101 内線 3585

THIS PAGE BLANK (USPTO)